



Deployment Guide for Cisco Unified Communications Domain Manager 8.1.4 ER2

First Published: 30 April, 2014

Last Modified: 30 October, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED 'AS IS' WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Contents

Preface	17
Introduction	17
Typographic Conventions	17
Provisioning	18
Provisioning Overview	19
Provisioning Steps	19
Accessing the system and initial setup	22
Prerequisites	22
Overview of the system interface	22
Transactions	23
Search functionality	27
Help functionality	27
Keeping your system secure	27
Overview of Users	29
Logging In	30
Changing Your Password	32
Creating a New super-user Account	32
Managing Your Administrator Account	35
Configuring Resources	36
Setup of Base Resources	36
Adding a CTI Manager Group	89
Adding a CTI Manager Group	89
Modifying a CTI Manager Group	90
Application User Management	91
CCM Server Configuration	94
Selecting the Server Type to Add	94
IP PBX Server	95
DHCP Server Management	96
TFTP Server Management	98
Voicemail Gateway Management	99
IP Edge Device Management	101
Console Servers and Services	102
Music Server Management	105
SMTP Server Management	107
Conference Server Management	108
Transcoder Server Management	111
Annunciator Server Management	113
Media Termination Point Management	128
Directory Server Management	129
Directory Service Management	130
Emergency Responder Management	132

IVR Server Management	137
SIP Application Servers	138
Hardware Group Management	143
CCM Media Resource Group Management	149
Loading a PGW	154
Loading a Cisco Unified Communications Manager (Unified CM) Cluster(s)	154
Provider Configuration	154
Legacy PBX Configuration and Management	154
Adding an IOS Device	154
Unmanaged PBX Devices	156
Adding the Unmanaged PBX to a Hardware Group	159
Adding an Unmanaged PBX Location(s)	159
Adding PSTN Published Numbers	159
Creating and Managing E164 Numbers	159
Adding Emergency Published Numbers	159
Provisioning Cisco Voice Messaging Services	160
Provisioning Cisco Unity Connection	160
Provisioning Cisco Unity	161
Cisco Unity Connection Auto Attendant Support	170
Enable the IVR role on Cisco Unity Connection	170
Auto Attendant Services	172
Location Auto Attendant Services	175
Cisco Unity Connection AA Specific Functionality Setup	176
Provisioning the Local PSTN Breakout Support	176
Netwise	178
Add a Netwise Cluster	178
View and Modify a Netwise Cluster	179
SIP Normalization Scripts Management	180
Associating the SIP Normalization Script to a Connection	183
Modifying the Trunk Details of a Managed-to-Managed Connection	183
Provisioning Other System Features	184
AutoCCMNewPhone Feature	184
Moving Phones between Location Subnets	187
Configuring Cisco Unified Communications Manager and the System	187
Key System Functionality	190
Add Users and Services	199
Adding End Users and Adding (Associating) the Required Services/Devices	199
Important Points to Know About Users and Services	199
Pre-requisites	200
Using the GUI	200
Using the Bulk Loader	201
Related Topics	202

IOS Gateways	202
IOS Device Management	205
Adding an IOS Device	205
Modifying an IOS Device	208
Device Roles	209
Media Service Management	264
Configure Per-Port COS for Emergency Calls from Analog Ports	264
Activate Per-Line COS for Analog Gateways	265
Supplementary Services on Analog Gateways	266
Enabling Supplementary Services	266
Analog Port Management	268
Register an Analog Line with an Analog Port	271
SCCP Supplementary Features	272
Valid Analog Line Features	272
Key Sync Features	273
IOS Commands	273
Download Command List	284
Exporting IOS Commands	284
PGW Pre and Post Functions	289
Supported MML Scripts	289
Transaction Failures and Rollback	289
Legacy Gateways	290
Search Functionality	290
Adding an IOS Device	290
Location Local Gateway Provisioning	301
The Local Gateway Index	301
Initial Provisioning of Dial Plan	301
Modification of the Current Dial Plan	302
Activation of Additional Ports/Gateways	303
Deactivation of Ports	303
Removal of Dial Plan	304
Transit Switch Management	304
PGW Server Management	306
HSI Management	312
Transit/Transit Server Management	318
Transit/Voicemail Server Management	319
Transit/Gatekeeper Management	320
Transit/IPPBX Server Management	321
PBX Server Management	322
IPPBX/Gatekeeper Management	323
IPPBX/Transit Management	324
IPPBX/Emergency Responder Server Management	325
IPPBX/Conference Management	326

IPPBX/Transcoder Management	327
IPPBX/TFTP Management	328
IPPBX/Voicemail Management	329
IPPBX/Third Party SIP Management	330
IPPBX/Location Management	331
Call Routing Connections	332
IPPBX/Contact Center Management	346
Device Sets	347
Connecting an Unmanaged Legacy PBX to another PBX	349
TDM Connectivity via an MGCP Gateway from a Leaf Cluster	349
IP Connectivity using H323 Trunks from a Leaf Cluster	351
IP Connectivity using SIP Trunks from a Leaf Cluster	351
Call Routing	352
Defining Call Routing Types in the system	352
Associate Call Routing Types to Country	352
Applying Call Routing at Location Level	353
Local Gateway Port Call Routing	354
Bulk Loader and Model Loader Changes	355
The Survivable Remote Site Telephony (SRST)	355
SRST Role	355
NAT for Gateways	359
NAT of Gateway Address to Unified CM	360
NAT of Unified CM Address to Gateway	360
Guidelines for usage based on specific NAT configuration	360
PGW Export Tool	361
Supported Transactions	361
Activating the PGW Export Functionality	362
Exporting MML and Times Ten data	362
AssociateFNN	363
Cloned Line (Multiline) Functionality	364
Support for Cisco Analog Telephone Adaptors (ATA)	368
Support VIA SIP	368
Mobility Connect	369
Versions	370
Required Plug-ins	370
Configuring Mobility Phone Type Integration	370
Eventing	370
Licensing	372
Enabling/Disabling License Types	372
Viewing Available Licenses	374
Refreshing the <i>Location License Management</i> page	374
Requesting a Quote For License Updates	374
Submitting an Order	375

Meet-Me	376
Adding a Meet-Me Number	376
Managing a Meet-Me Number	377
Bulk Loading Meet-Me Numbers	377
Managing Phone Services	378
Enabling IP Phone Services in a Feature Group	382
IP Phone Service subscription management	383
Modify container details	383
IP Phone Service Subscription Management for Individual Devices	384
Manage IP Phone Service Subscriptions	385
Leaf Cluster Overview	386
PBX to PBX Connection management	387
SME Clusters	392
Cisco Unified CM Session Manager Edition	392
Managing SMEs via Bulk Loaders and Models	392
Managing SMEs via the system GUI	392
Idle URL Management	400
Adding a Service Type for an Idle URL	400
Managing the Idle URL Setting via the Feature Group	401
Managing the Idle URL Individually for the Phone	401
Extension Mobility Cross Cluster (EMCC) Configuration	401
EMCC Use Case	402
EMCC Server Setup	402
Home Cluster Setup	403
View EMCC Configuration	412
EMCC Group Management	413
Enabling/Disabling EMCC using the Bulk Loaders	415
Extension Mobility Location Group Management	415
Adding an Extension Mobility Location Group	416
Modifying an Extension Mobility Location Group	416
Mobile Connect/Single Number Reach (SNR)	417
Adding a Single Number Reach Remote Destination	418
Setting and Resetting a Primary Device for an End User	424
Modifying a Single Number Reach Remote Destination	425
Checking the CCM Data	425
Mobile Identity Management	425
Synchronization with Cisco Unified Communications Manager (Unified CM)	429
Subnets	429
NAT and PAT	430
Adding and Managing Subnets	430
Edge Devices	431
Extension Management	431
Managing Available Internal Numbers	431

Manage Extensions (Internal Numbers) using Bulk Loaders	432
Connect Location	432
Via the <i>Location Administration</i> Menu	432
Via the <i>Operations Tools</i> Menu	433
Associate PSTN Number Ranges and Connect Location	434
Feature Display Policies	434
Adding a Feature Display Policy	435
Adding Feature Display Policy Groups	437
Feature Display Policy Management	438
Assigning Feature Display Policies	438
Shared SLC	439
Adding a Linked Location Parent	440
Converting a Standard Location to Linked Location Parent	440
Converting a to Linked Location Parent a Standard Location	441
Adding a Linked Location Child	441
Reassigning the Linked Location Parent Role in Linked Locations	441
Hunt Group/Number Groups for Linked Location	441
Location Level Operations Tool to Delete Lines of Different Linked Location from the Number Group	442
Bulk Loading Linked Locations	442
CTI/TAPI Management	442
Adding CTI Route Points/ CTI Ports	442
Line Setting Information	445
Modifying CTI Route Points/ Ports	451
Transit Deferral	452
Enabling Deferral	452
Error Handling	452
Affected Transactions	453
Session Border Controllers	453
Session Border Controller Management (SBC)	453
Manage Session Border Controller	455
SBC Connected Locations	458
Manage SBC Interfaces	459
SBC Connectivity	461
Allocating Location to the Hardware	463
SBC and OCS Management	463
Activating an SBC	463
Deactivating an SBC	464
Modifying the Call Limit and OCS Numbering	464
Access Profiles	465
Additional Restrictions	467
Adding an Access Profile	470
Modifying and Deleting Access Profiles	475

Defaults for Access Profiles	475
Security profiles	489
Security profile management	489
Adding a security profile	490
Modifying and deleting security profiles	493
Brand Management	494
Importing a Brand	495
Brand Editor Overview	496
Deploying Brands	498
Feature Group Administration	500
Feature Group Management	500
Features Available when Adding or Modifying a Feature Group	505
Device Group Management	513
Operations Tools	515
Transaction Log and Search Report	515
Using the transaction search screen	515
Access to Transaction Logs for End Users	516
Bulk Administration	516
Bulk Administration Preview and Add	518
Bulk Administration file formats	520
Common Bulk Administration tasks	520
IVR/Transit Server Management	525
Transaction Auditing	526
Management of Transaction Auditing	526
Transaction Auditing Application	528
Transaction Details	529
Billing Codes (Client Matter Codes)	530
Quick Search	534
Search For	534
Finding Locations	535
Finding Extensions	536
Finding Phones (Device Name)	538
Phone with Extension	539
Phone with DDI	539
Phone with User	539
Find a Phone in the List	539
Finding a User	541
Bulk and Model Loader Functionality	543
Model Management	543
iFINT Migrate Feature	549
Number Construction Rules	549
Activating the iFINT Migrate Functionality	549
iFINT Migration History Logs	550

Dial Plan Terms	550
Number Construction	551
Details	551
Codec Selection	551
Dial Plan Rules	551
Internal Number Format	552
Internal Number Display Rules	553
RID Type Selection	553
Dial Prefixes	553
Format of External Phone Number Mask on Unified CM	554
Format of IPPBX Configured Internal Number	554
Format of Voicemail Configured Pilot Number	555
Format of Voicemail Configured Mailbox Number	555
Configurable FINTs	556
Recommended Dial Plan Configuration by Solution	556
HCS Solution	556
Device Pool Templates	558
Adding a Device Pool Template	559
Modifying a Device Pool Template	561
Feature Configuration Templates	562
End User Migration	563
End User Migration Preview	565
Number Translations	565
E164 Numbers	570
Pre-requisites for adding E164 numbers	571
Using the GUI	572
Using Bulk Loaders	579
Related topics to E164 numbers	580
Forced Authorization Codes	581
Add FAC	582
Assign FAC	583
Release FAC	583
Delete FAC	583
Customer Specific Button and Softkey Templates	583
Button Group Management	583
Emergency DDI	587
Country Setting	587
Customer Setting	587
Location setting	588
FNN Range Setting	588
Authentication Management	588
Enable External Authentication in Security Profile	589
Authentication Management steps	590

LDAP Integration with Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection	594
Limitations	594
Configuring LDAP Integration	595
Cisco Unified Communications Manager IM and Presence (IM and Presence) Server	603
Managing a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server	603
Connect an IM and Presence Server to an IPPBX	607
Cisco Unified Communications Manager IM and Presence (IM and Presence) Manual Configuration	608
Driver_Presence Implementation of the <i>VerifyCUPCapabilities</i> Transaction	610
Service Profile Management	610
UC Central	618
Provisioning UC Central	619
Enabling a User's extension as a UC Central extension	623
Disabling a User's extension as a UC Central extension	624
Deactivating a User's UC Central connection	624
Voicemail Services Management	624
Add a Voicemail Service	625
View or Delete a Voicemail Service	625
Conferencing	626
Conference Service Management	626
WebEx Conferencing	633
Single Inbox	637
Activating Single Inbox	637
Selecting a Unified Messaging Service for Single Inbox	638
Modifying the Unified Messaging Service for an Existing Voicemail Account	638
Corporate Directory Partitions	638
Assigning a Directory Partition	640
Hide a Shared line from Corporate Directory	640
CLI Group Management	641
Codecs	646
Default Cisco Unified Communications Manager (Unified CM) Codec Values	647
Audio Regions	647
Bulk Loading Codecs	649
Automatic Codec Scaling	649
Contact Centers	650
Contact Center Servers	650
Contact Center Service Management	654
Recording Profiles and Recording Options	661
Migration Concerns	662
Service Inventory: Billing	662
Caveats	662
ASCII Fields	662

Enabling ASCII fields in the Feature Display Policy	663
Enabling ASCII fields in the Feature Group	663
Phone Lines	663
CTI Route Points	664
CTI Route Ports	664
Mobility	664
Busy Lamp Fields	665
Speed dials	665
Bulk loading ASCII values	666
Importing Device Specific Settings	666
Importing Advanced Phone Features	666
Feature Group setting for Advanced Phone Settings	668
Feature Display Policy Setting for Advanced Phone Settings	668
Managing Advanced Phone Settings for a Device	668
Managing Advanced Phone Settings in Self Care	669
Specifying Advanced Phone Settings when Bulk Loading Phones	669
Importing Advanced Phone Settings for Existing Devices via CLI	669
Music on Hold Track Management	669
Adding a MoH Track	669
Viewing and Modifying MOH Tracks	670
Provider Administration	671
Adding a Service Provider	672
Modifying and Deleting a Service Provider	672
International Gateway Usage	673
Advanced Telephony Settings	674
Delete a Service Provider	675
Provider Country Management	675
Adding a country to a Provider	676
View and delete a country withing a Provider	676
Feature Group Template Management	677
Add a Feature Group Template	678
Viewing and Modifying Feature Group Templates	678
Managing PBX Templates	679
IP Addresses and Phones	681
IP Inventory Management	681
Add Phones to the Phone Inventory	684
Site Code Management	685
Add a Site Code	685
Provider Level Voicemail Service	686
Setting the Provider Preference to use Provider Level Voicemail Service	686
Adding a Provider Level Voicemail Service	686
Add Voicemail Service Pilot Number	687
Voicemail Template Management	687

Voicemail Template Restrictions	688
Associate a Number Range	689
Adding a Location Voicemail Profile	689
Adding Administration Users	689
Allocating E164 Numbers and Phones to Specific Locations	692
Allocating E164 Numbers to Locations	692
Allocating Phones to a Location	693
Reseller Administration	694
Resellers	694
Adding a Reseller	694
Managing a Reseller	695
Managing Reseller Administrators	696
Adding an Administrator	696
Modifying an Administrator	699
Reset an Administrator's Password	699
Deleting an Administrator	699
Customer Administration	700
Customer Management	700
Add a Customer	701
View and Modify a Customer	703
Advanced Customer Management	703
Advanced Telephony Settings	704
Customer License Management	708
Preferences	710
Deleting a Customer	711
Copying Feature Groups	712
Activate User Roaming	712
Activate User Roaming via Preferences	712
Activate user extension mobility via feature groups	713
Activate user extension mobility for customers	713
Overview of Extension Mobility Cross Cluster for Customers	714
Division Administration	716
Add a Division	716
Modifying a Division	717
Building Administration	722
Managing Buildings	722
Adding a Building	723
Managing Buildings	724
Site Code Management for Buildings	727
Managing Building Voicemail Services	728
Voicemail Pilot Number Management	730
Selecting the Required Voicemail Service Profile	731
Manage Building Auto Attendant Services	732

Allocating E164 Numbers to the Voicemail and Auto Attendant Services	732
Feature Group Management	734
Customer Building Management	736
Manage Building Preferences	739
Managing a Building Preferences and Settings	739
Managing a Building's Details	739
Allocating an E164 Number Inventory to a Building (Location)	739
Allocating a Phone to a Building (Location)	740
Building Voicemail Service - E164 Number Management	740
Adding an Emergency Published Number	742
Assigning an E164 Number Range to Internal Numbers	742
Managing Users and Phones	743
Operations Tools	743
Location Administration	744
Managing locations	745
Location Administration - Quick Reference	746
Hierarchy Levels	746
Finding a location	747
Deleting a Location	748
Adding a location	749
Managing a Location	757
Location Main Page	758
The PBR Process Using Bulk Loaders	789
The PBR Process Using the system GUI	795
Phone Management	803
Managing the Phone	806
Manage Lines	810
Manage Speed Dials	814
Busy Lamp Fields	815
Manage Service URL	817
Login User	818
Phone Alerting Names	818
Contact Center Agent Lines	819
Replace a Phone	819
Unregistering / Deleting a Phone	820
Location Administration Tools	821
Unmanaged Locations	822
Adding an Unmanaged PBX	822
Adding a Hardware Group for Unmanaged Locations	822
Adding an Unmanaged Location	823
Location Administration for Unmanaged Locations	823
Allocated Connectivity for the Location	823
Resource Management	823

Managing Available Internal Numbers	824
External numbers	826
Phone Inventory	830
Managing Users	839
Find a User	839
Delete a User	841
Add an End User	842
Manage an End User	846
Reset User's Password	850
Unlocking a locked User account	851
Reset User's Phone PIN	851
Associate/Unassociate (or Delete) Device with/from User	852
Extension Mobility Profiles	854
Manage Voicemail Accounts	867
Create Voicemail Account	870
WebEx Conferencing	873
UC Central	874
Administration Users	876
Managing Numbers	884
Telephony Management	884
Number Group Management	897
Hunt Group Management	901
Pickup Groups	905
Presence Monitoring	910
Location License Management	911
Self Care Skinning	914
Theme Management	914
Appendix	918
Available Server Fields	919
ATA Device Parameters	926
Basic Device Parameters When Using SIP	926
Advanced Device Parameters When Using SIP	926
Hardware Devices Supported	927
Phone Types	927
Expansion Modules	931
Miscellaneous Devices	931
IOS Gateway Hardware	932
Available Preferences and Settings	934
Using System Preferences	934
Location Preference and Settings	935
Provider Preference and Settings	937
Division Preference and Settings	942
Customer Preference and Settings	942

Reseller Preferences and Settings	946
System Preference and Settings	946
Building Preferences	949
Dial Plan Preference and Settings	950
Operations Tools	950
Upgrade Limitations	966
Unified CM Group Allocation Logic	967
Overview	967
Adding a New CCM Group to the Cluster	967
Caveats and Limitations	968
Glossary	968

Preface

Introduction

The system is an Operational Support System (OSS) designed to automate the configuration of a unified communications infrastructure and manage all of the related business services.

The system is a management tool designed to assist both service providers and enterprises with the management of their voice services, resources and underlying infrastructure. The system provides both:

- A complex, modeling and work flow engine for centralized service management and automated infrastructure configuration.
- A web-based, simple-to-use, front-end that simplifies the business processes required for managing Unified Communications services.

This system supports various deployments/solutions including HCS and Large Enterprise (LE). This document describes the product in general and is not specific to a particular deployment/solution. Information may vary slightly depending on the installation environment.

Typographic Conventions

The following typographic conventions are used in this document:

Item	Character format	Example
Buttons	Bold	Click the Enter button.
Checkboxes	<i>italic</i>	Select the <i>Country</i> checkbox.
Dialog boxes menu items, tab names, radio buttons	<i>italic</i>	Select the <i>Configuration</i> option, or select the <i>Parameters</i> tab.



CHAPTER 1

Provisioning

Provisioning Overview	19
Provisioning Steps	19
Accessing the system and initial setup	22
Prerequisites	22
Overview of the system interface	22
Transactions	23
Search functionality	27
Help functionality	27
Keeping your system secure	27
Overview of Users	29
Logging In	30
Changing Your Password	32
Creating a New super-user Account	32
Managing Your Administrator Account	35
Configuring Resources	36
Setup of Base Resources	36
Adding a CTI Manager Group	89
Adding a CTI Manager Group	89
Modifying a CTI Manager Group	90
Application User Management	91
CCM Server Configuration	94
Selecting the Server Type to Add	94
IP PBX Server	95
DHCP Server Management	96
TFTP Server Management	98
Voicemail Gateway Management	99
IP Edge Device Management	101
Console Servers and Services	102
Music Server Management	105
SMTP Server Management	107
Conference Server Management	108
Transcoder Server Management	111
Annunciator Server Management	113
Media Termination Point Management	128
Directory Server Management	129

Directory Service Management	130
Emergency Responder Management	132
IVR Server Management	137
SIP Application Servers	138
Hardware Group Management	143
CCM Media Resource Group Management	149
Loading a PGW	154
Loading a Cisco Unified Communications Manager (Unified CM) Cluster(s)	154
Provider Configuration	154
Legacy PBX Configuration and Management	154
Adding an IOS Device	154
Unmanaged PBX Devices	156
Adding the Unmanaged PBX to a Hardware Group	159
Adding an Unmanaged PBX Location(s)	159
Adding PSTN Published Numbers	159
Creating and Managing E164 Numbers	159
Adding Emergency Published Numbers	159
Provisioning Cisco Voice Messaging Services	160
Provisioning Cisco Unity Connection	160
Provisioning Cisco Unity	161
Cisco Unity Connection Auto Attendant Support	170
Enable the IVR role on Cisco Unity Connection	170
Auto Attendant Services	172
Location Auto Attendant Services	175
Cisco Unity Connection AA Specific Functionality Setup	176
Provisioning the Local PSTN Breakout Support	176
Netwise	178
Add a Netwise Cluster	178
View and Modify a Netwise Cluster	179
SIP Normalization Scripts Management	180
Associating the SIP Normalization Script to a Connection	183
Modifying the Trunk Details of a Managed-to-Managed Connection	183
Provisioning Other System Features	184
AutoCCMNewPhone Feature	184
Moving Phones between Location Subnets	187
Configuring Cisco Unified Communications Manager and the System	187

Provisioning Overview

This section outlines the steps that need to be followed to successfully deploy the system. This is meant to be a high level overview of the provisioning process. Follow the relevant links for further information on each step. Certain deployment tasks need to be carried out manually while other tasks can be carried out using the system's bulk loader and configuration model functionality. Where possible, the bulk loader and manual steps have been outlined.

Provisioning Steps

Procedure

To provision the system:

Step 1 Configure the Cisco Unified Communications Manager (Unified CM) and install the system:

- a** Make all relevant changes to the Unified CM for the system. For more information, see the standalone CUCM Build Guide.
- b** Complete the configuration of any hardware that requires configuration prior to the installation of the system, for example Cisco Unity. Please consult the relevant standalone guide for information on configuring specific hardware.
- c** Install the system on the required server. For more information, see the System Installation guide or contact your dedicated support person.

Step 2 Log in to the system:

- a** Log in to the system using the default account
- b** Create a new super-user user account

For more information, see [Logging In on page 30](#).

Note

Bulk loaders can also be used to load much of the resource data mentioned in steps 3 and 4. Refer to the Bulk Loader Guide for more information if required.

Step 3 Configure the required resources:

- a** Configure resources such as phone types, service types and available countries
- b** Add a dial plan
- c** Create a hardware set and connect it to a dial plan
- d** Load the relevant dial plan models
- e** Add a provider(s) and all required resources (number resources, phone resources etc.)
- f** Create and associate all required gatekeepers
- g** Create and associate any Cisco Packet Data Network Gateways (PGWs)
- h** Create and associate any Cisco Unified CM clusters
- i** Create and configure a DHCP server(s)
- j** Create and configure any required Trivial FTP (TFTP) servers
- k** Create and configure any IP Edge devices
- l** Create and configure any required Music on Hold (MOH) servers
- m** Create and configure any required conference servers
- n** Create and configure any required transcoder servers
- o** Add any required hardware groups
- p** Add any required media resource groups, media resource group lists and Unified CM groups (also referred to as CCM groups)
- q** Load any Cisco PGW and/or Unified CM Clusters

For more information, see [Configuring Resources on page 36](#).

Step 4 Configure required providers:

- a** Add required countries
- b** Add required area codes
- c** Create an E164 number inventory
- d** Create a phone inventory
- e** Create required resellers
- f** Add required customers
- g** Add required media services
- h** Add required feature groups
- i** Add required divisions
- j** Add required locations
- k** Allocate E164 numbers and phones to the relevant locations
- l** Add PSTN published numbers to the relevant locations
- m** Add emergency published numbers to the relevant locations
- n** Allocate E164 number ranges to internal numbers within the relevant locations
- o** Register required phones within the relevant locations
- p** Add required end users to the relevant locations

For more information, see [Provider Configuration on page 154](#).

Step 5 Configure any Legacy PBX's (Optional):

- a** Create any required Internetwork Operating System (IOS) devices
- b** Add required unmanaged PBX locations
- c** Add required PSTN published numbers
- d** Create and configure required media gateways
- e** Create an E164 inventory
- f** Add Emergency Published Numbers
- g** Allocate E164 number ranges to internal numbers

For more information, see [Legacy PBX Configuration and Management on page 154](#).

Step 6 Configure Unified Meeting Place (Optional):

Configure Unified Meeting Place in the system.

Step 7 Configure and deploy Cisco Unity (Optional):

Configure and deploy Cisco Unity within the system. For more information, see [Provisioning Cisco Voice Messaging Services on page 160](#).

Step 8 Configure Local PSTN Breakout Support (Optional):

Configure local PSTN breakout support within the system. For more information, see [Provisioning the Local PSTN Breakout Support on page 176](#).

Step 9 Configure and deploy Netwise (Optional):

Configure and deploy Netwise within the system.

Step 10 Configure NAT/PAT (Optional):

Configure NAT/PAT within the system.

Step 11 Configure and deploy a Cisco Emergency Responder (Optional):

Configure and deploy required Cisco Emergency Responders within the system.

Step 12 Configure and deploy a Cisco Unified Contact Center (Optional):

Configure and deploy required Cisco Unified Contact Centers within the system.

Step 13 Complete any custom configuration:

Complete any custom configuration required for your deployment.

Accessing the system and initial setup

This section covers logging into the system. You will need to log into the Cisco Unified Communication Domain Manager (CUCDM), also commonly referred to as the 'system', to manage both the telephony profile of end user's, and to manage the administration of your organization's communication system. See also: [Logging In on page 30](#).

Prerequisites

This section presumes the following:

- The system has been successfully installed, if not, please refer to the System Installation guide.
- Users of this guide have access to a computer that is able to access the system's web-based GUI.
- The users of this guide have a basic understanding of telecommunications terminology and principles. See [Glossary on page 968](#) for more information.

Overview of the system interface

The following standards are used within the system's administration interface:

- Browsing the system

The easiest way to browse the system is via the navigation menu on the left. The navigation menu is accessible from any page within the system. To return to the previous screen, use the "Return to....." link (if available) at the bottom-left of the screen. If the "Return to...." link is not available, you can use your browser's back button to view previous pages; however, the web page may expire (time-out), and you will lose any information that has not yet been committed to the system.

- Hyperlinks

All links, referred to in documentation as active text links, have a blue font color.

- Fields and options

Mandatory fields and options are indicated using an asterisk (*).

- Transaction status

After completing a task, the system presents a summary of the transactions processed. This summary includes the status of the processed transactions as well as any relevant explanations.

- Committing changes

Changes to a page are not saved until you click the **Add**, **Submit**, **Update** or **Modify** button. Browsing off a page without selecting one these options will result in the loss of any uncommitted information.

- Help

Help is available from every page within the system. Selecting the *Help* active text link in the top left hand corner of the page launches a context sensitive help screen. Selecting the *Help* link from the main menu launches a generic help screen. For more information, see [Help functionality on page 27](#).

- Searching in the system

The search functionality is available from each page of the system by selecting the *Quick Search* link in the top right hand corner. This enables you to search for entries such as phones, extensions, and user accounts. For more information, see [Quick Search on page 534](#).

Transactions

Transactions are a record of the system performing all of the configuration processes in response to administrators and users performing the day-to-day tasks in the system. The system tracks all of these transactions and sub-transactions and enables administrators to access these records.

Transaction status

Transaction statuses summarize the state of a requested action (transaction). Transactions often consist of multiple sub-transactions; the status of these sub-transactions is also reported by the system.

Transactions can be in three key states:

- *Request being actioned:*

The system is busy processing your request, it is advisable to wait and let the system finish processing your request before proceeding.

- *Request Failed:*

The system was unable to process your request/transaction. Analyze the error message provided and correct the problem before processing the request again.

- *Request Succeeded:*

Your request was actioned successfully.

Note

- To continue using the system while transactions are running, select the *Return To* link.
 - For further information on why transactions are failing, administrators can use the *Manage Transactions* page to view details of all transactions and sub-transactions.
-

Transaction management

Administrators must access the transaction log when they troubleshoot the system. The transaction log provides a chronological record of all the failed and successful activities.

The transactions are recorded in detail (multiple sub-transactions usually make up each transaction), in chronological order, linked to each user. Unsuccessful transactions show the roll-back of the earlier sub-transactions.

Note

Administrators are able to access the transaction logs and search for transactions executed by users within their areas of responsibility. Super users have access to additional transaction tools.

Procedure

Viewing transactions

- Step 1** To view transactions, browse to *General Tools > Transactions*.
- Transactions are listed in a table with the Id number, the User ID, Action, Status and Message (a brief description).
- Step 2** To view the sub-transactions of a transaction, select the ID number in the left hand column. The *Transaction Inquiries* screen lists all the sub-transactions for the primary transaction.
-

Procedure

Searching the transactions log

Search the transaction log by selecting required search criteria in the *Search By* drop-down list. Options include:

Criteria	Description
All Transactions (Message)	Returns search results for all transactions processed
My Transactions (Message)	Returns search results for the user currently logged in
Selected User	Returns search results for the user selected from the drop-down list
Failed Transactions	Returns search results for transactions that failed
In Progress	Returns search results for transactions that are currently in progress
Not Processed	Returns search results for transactions that have not been processed
Succeeded	Returns search results for transactions that succeeded
After Transaction #	Returns search results for transactions submitted (post) after the transaction number specified
Before Transaction #	Returns search results for transactions submitted before (prior to) the transaction number specified.
Canceled	Returns search results for canceled transactions
WS UUID	Returns search results for the WS UUID specified.
WS External UUID	Returns search results for the WS External UUID specified.
WS External Reference	Returns search results for the WS External Reference specified.
Transaction ID	Returns search results for the Transaction ID specified.

Use two additional filters (checkboxes) if required.

Exclude Web Transactions: Excludes all transactions executed by the *bvsm* user from the search results. (Show only transactions executed from a phone.)

Exclude End-User Transactions: Excludes all transactions executed by end-users (level 6) from the search results.

To search the transaction log:

- Step 1** Select the required option from the *Search by* drop-down list.
- Step 2** Select the number of search results that you would like returned from the *Max results* drop-down list.
- Note**
Selecting *unlimited* may make the browser unresponsive.
- Step 3** Select the relevant *time period* from the drop-down list.
- Step 4** Enter a *search string* in the text box to search the transaction *Message*.
- Step 5** Select the *Exclude Web Transactions* and/or **Exclude End-User Transaction** filter check-boxes if required.
- Step 6** Click the **Search** button.

All transactions matching your search criteria are returned in a list.

Note

For Super User features, please see [Super user features on page 25](#).

Super user features

Transaction roll-back. The system rolls back certain changes if a failure occurs within a transaction. There is however no rollback within the actual sub-transaction that fails. The system rolls back any successful sub-transactions prior to the sub-transaction that failed. However, it does not roll back any actions within the actual sub-transaction that caused the failure. For example, within *AddLocation* there are a number of AXL calls within each sub transaction; if a call fails, the successful AXL calls within the same sub-transaction are not rolled back. However, all sub-transactions prior to the failed sub-transaction are rolled back.

As mentioned above, configuration applied within a Child transaction is not rolled back. This includes the device drivers that are child transactions for example *Driver_IPPBX*. Therefore, if a call to the device driver includes several configuration commands/API calls then any successful commands/APIs are not undone if a later API/command fails from the same *Driver_IPPBX* transaction.

The device being configured and its capabilities affect the roll-back behavior as noted below. For the key devices provisioned:

- **Cisco Unified Communications Manager (Unified CM) (Driver_IPPBX)**

For Unified CM this is an AXL API call. If the API command completes successfully, then the configuration is applied. Transactions with multiple API calls from the same *Driver_IPPBX* could result in some configuration being applied and not rolled back. Typically this is overwritten when the transaction is successful after resolving the error condition. One exception is *AddLocation* which appends a database to the end of element names. If the transaction fails, then when the location is added the database-id increments.

- **PGW (Driver_Transit)**

Because the PGW works by opening a configuration session, applying the commands and then deploying it, rollback is not a concern here. If there are any errors in the commands then the config is not deployed.

- **PGW Times Ten (Driver_TimesTen)**

This calls a program on the PGW which does the changes in the database. The program handles the roll-back for any failures in the individual entries. If multiple calls to the program are made from the same child transaction then roll-back between these is not handled - this would occur if the batch size was exceeded and the commands needed to be broken up into several calls. Transactions like AssociateFNN are likely candidates for exceeding the batch size.

- **SME (Driver_Transit)**

Same as for the Unified CM description above.

- **Unity Connection (Driver_Voicemail)**

This is done through an API interface; when the API call is successful the configuration is live. If there are multiple API calls in a single Driver_Voicemail call then this successful command will not be rolled back if one fails.

- **IPUnity (Driver_Voicemail and AutoAttendant)**

This is done through an API interface so when the API call is successful the configuration is live. If there are multiple API calls in a single Driver_Voicemail call then this successful command will not be rolled back if one fails.

- **IOS Device (various - gateway, etc)**

This is a command interface essentially typing the commands into the device via a SSH session as an admin would. So the commands take effect immediately in the IOS device. If a command fails, the previous commands are not undone. Typically this will be overwritten when the transaction is successfully completed after resolving the error condition.

- **Presence (Driver_Presence)**

Same as for the Unified CM description above.

- **Webex (Driver_Conference)**

This is done through an API interface; when the API call is successful the configuration is live. If there are multiple API calls in a single Driver_Conference call then this successful command will not be rolled back if one fails.

Procedure

Canceling transactions

The system enables administrators to cancel transactions that are queued or processing. Each transaction in the system is divided into steps. If the **Cancel** button is clicked, the system stops processing the transaction at the end of the next step in the selected transaction. If the transaction has not started, the transaction is canceled. The system rolls back the transaction steps and undoes all the actions taken for the selected transaction. This results in the selected transaction being rolled back and the system being left in a stable state.

To cancel a transaction:

- Step 1** Browse to *General Tools > Transaction*.
- Step 2** Locate the transaction that you would like to cancel using the search functionality (see [Search functionality on page 27](#)).
- Step 3** Click the **Cancel** button adjacent to the transaction that you would like to cancel. The transaction is canceled.

Procedure

Replay transactions

Super users can replay transactions as follows:

- Step 1** Browse to *General Tools > Transaction*.
 - Step 2** Browse or search for the transaction that you would like to replay using the search functionality (see [Search functionality on page 27](#)).
 - Step 3** Click the **Replay** button adjacent to the transaction that you would like to replay. The transaction is replayed.
-

Search functionality

Click the *Quick Search* text link at the top right hand side of a user interface page to open the *Quick Search* page.

This page provides a quick and efficient search mechanism for entries of various types from a single page in the system without the need to navigate up / down / the system hierarchy tree via the menu. The Quick Search options and results to which you have access are determined by the access privileges associated with the user account that you used to log into the system.

For further information on using the Quick Search functionality, see [Quick Search on page 534](#).

Help functionality

There are four ways to access help:

- **Context sensitive help:** Select the *Help* link at the top left of the screen. The system displays context specific help window.
- **Browsing the index:** If you know what section of the system you are interested in, select the *Help Index* active text link from the Menu to open a separate Help window. Browse to the relevant section on the Index tab (table of contents).
- **Searching help:** If you know the concept or topic you are interested in, select the *Help Index* active text link from the Menu to open a separate Help window. Enter the required search string, for example, "Adding a phone" and click the adjacent **Search** button. More information on searching is available below.

- **Browsing the glossary:**

If you are looking for the meaning of a term or acronym, select the *Help Index* active text link from the Menu to open a separate help window. Select the *Glossary* tab and click on the required term for the definition.

Keeping your system secure

While the system is a safe and secure product, the security of the system is ultimately determined by the behavior and habits of the users. Steps you can take to ensure the continued security of your system include:

- Effectively securing user passwords
- Maintaining user access rights at a "no higher than each user needs" security level

Securing passwords and PINs

It is important that users keep their PIN and password as secure as possible.

Hints for managing your PIN and password:

- Users should not share their PIN numbers or passwords with other users.
- Users should not write down their PIN numbers or passwords or store them in an obvious place, such as a pin-board or diary.
- Users should not use pattern based or obvious passwords such as a birthday or the user's name.

The system places a number of limitations on the type and nature of passwords that can be used; this is to ensure that passwords are kept as secure as possible. Some of these parameters include:

- **Minimum length:**

Passwords have a minimum length of six (6) characters.

- **Difference from previous passwords:**

Passwords must be different to other passwords that have been used. Passwords similar or identical to previously used passwords are not accepted.

- **Specific characters:**

Depending on how your system has been configured, your password may need to contain a minimum number of specific characters such as upper case, punctuation, and/or numeric characters. See [Password length credits on page 28](#) for more information on password credits.

- **Dictionary terms:**

Passwords may not be based on dictionary words, terms, character or numeric sequences. For example: password, qwerty, 1234.

Depending on how the system is configured, users can be required to periodically renew their password. Once the expiry period has been reached, when a user logs in they are given a warning showing the number of days before their password expires. Failure to change a password within the expiry warning period results in the user's account being locked.

Password length credits

Note

- Regardless of the minimum specified password length, length credits specified or the number of special characters used in a password, passwords may not be less than six characters.
 - The system does not place the same restrictions on administrators when they change a user's password as when a user changes their own password.
 - All password length credit fields are mandatory.
-

The system utilizes a password length credit system to ensure that users achieve an acceptable level of password complexity. This system rewards users who include certain characters in their passwords by reducing their minimum password length relative to the number of special character included in their passwords. Special characters can include non-alphanumeric, upper-case and numeric characters. The system can also ensure that users include a minimum number of the above character types in their passwords.

A negative value for any of the *Length Credits* indicates a minimum number of characters of that type that must be included in the password. For example, if "-2" is specified in the *Credits for Digit* field, then a minimum of two digits (numerals) must be provided in the password.

A positive value for any of the *Length Credits* indicates that the use of that character in a password results in the minimum password length being decremented by the supplied value.

The minimum length of the password is calculated using the following formula:

Minimum length of Password field - Sum of all Length Credit fields = Minimum Password Length.

As long as the minimum password length is greater than 6, the minimum length of the password is decremented for each length credit value.

Passwords have a maximum length of fifty (50) characters.

Example 1. Examples

Scenario 1

Minimum Password Length is specified as 10 characters.

Digit Length Credits is specified as 1 and all other *Length Credit* fields are configured to 0.

The minimum length of any password that includes a digit (1, 2, 3, 4 etc.) becomes 9 characters.

Acceptable passwords include: wdctrfgh1 and 2prtetygh.

Scenario 2

Minimum Password Length is specified as 10 characters

Digit Credits field is specified as 1, the *Non-alphanumeric Credits* field is specified as 1 and all other *Length Credit* fields are configured to 0.

The minimum length of any password that includes a digit (1, 2, 3, 4 etc.) and a non-alphanumeric character (#, ?, ! etc.) becomes 8 characters.

Acceptable passwords include: d?ctrfh1 and pr!tety1.

Hierarchy Levels

A key aspect of security within the system is the use of access hierarchies to limit a user's access only to functionality they need. The following hierarchical levels are supported in the system (from the highest to the lowest user level):

- Provider
- Reseller
- Building
- Customer
- Division
- Location
- User (End user)

Overview of Users

The system contains two core types of users: end users and administrators.

Note

The system has two login interfaces: *End User Self Care* and *System Administration*. Only end users are able to log in via the *End User Self Care* interface and only administrators are able to login via the *System Administration* Interface. Ensure that you select the login interface that is appropriate to your user hierarchy (user security level).

Administrator user accounts have the following features:

- Administrators can manage their own accounts by selecting *My Account* on the *Menu*.
- Administrator accounts are managed on the User Management page via the *General Administration > Administration Users* menu.
- Administrators cannot log in to the *End User Self Care* interface.
- There are various hierarchies of administrator users such as location, customer and provider.

End user accounts have the following features:

- End users can manage their own accounts via the *End User Self Care* interface.
- End users accounts are managed on the User Management page via the *Location Administration > End Users* menu.
- End users cannot log in to the *System Administration* interface.
- Only one hierarchy is available for end user accounts.

The following table summarizes the differences between the two core user account types:

	End User Accounts	Administrator Accounts
Log in to <i>End User Self Care</i> interface	Yes	No
Log in to the <i>System Administration</i> interface	No	Yes
Access to the <i>My Account</i> menu	No	Yes
Users managed via <i>Location Administration > End Users</i> menu	Yes	No
Users managed via <i>General Administration > Administration Users</i> menu	No	Yes
Different hierarchies available, for example Location, Provider	No	Yes
User can be allocated a phone	Yes	No
User can view and modify other users	No	Yes

Logging In

This section covers logging in to the system and provides a brief introduction to user profiles. You must to log in to the system to manage both your own telephony profile and if you are an administrator, to manage your organization's communication system.

In some cases, you can perform self-administration of your profile and settings on the phone itself, but it is generally easier and faster to perform these tasks online via the graphic user interface (GUI).

- Pre-requisite

To access the system's web GUI, you are required to have access to a web browser. Supported browsers are:

- Mac 10.8 - Chrome 29, Firefox 23, Safari 6
- Windows 7 - Chrome 29, Firefox 23, IE10
- Windows XP - Chrome 29, Firefox 23, IE8

Note

The system does **not** support multiple logins per user in the same Web browser session.

To log in to the System Administration GUI

Procedure

Method 1: Using your standard username (shortname - no user group)

From the *Log In* screen:

- Step 1** Enter your standard username.
 - Step 2** Enter your password.
 - Step 3** Click the **Log in** button or press **Enter**.
 - Step 4** The main menu screen is displayed, which allows you to select the various administration options that you are authorized to access.
-

Procedure

Method 2: Using your full username (including user group)

Unique Username

An administrator that can add a customer can also specify a user group for that customer. All users created for that customer belong to the specified user group. Users that existed before the user group was specified automatically have their usernames changed to include the user group name. The current (standard) username is combined with the specified user group to create a unique username at customer level, for example username@usergroup.

Note

The unique username feature is available only in system version 8.0 and higher, and only to System-, Provider- and Reseller administrators.

From the *Log In* screen:

- Step 1** Enter your full username, for example username@usergroup.
 - Step 2** Enter your password.
 - Step 3** Click the **Log in** button or press **Enter**.
 - Step 4** The main menu screen is displayed, which allows you to select the various administration options that you are authorized to access.
-

Note

Alternatively, the user group can be specified in the login URL (see Method 3 below), which allows you to login with your standard username only.

Procedure

Method 3: Specifying your user group in the login URL

- Step 1** Type the following **URL** into your web browser: `https://"address"/LOGINBVSM?usergroup="UserGroup"` , for example `https://192.168.0.0/LOGINBVSM?usergroup=location1group`, and then press **Enter**.

Note

At this point you can create a bookmark to this page to facilitate an easier login process for future logins.

- Step 2** Enter your standard username.
- Step 3** Enter your password.
- Step 4** Click the **Log in** button or press **Enter**.
- Step 5** The main menu screen is displayed, which allows you to select the various administration options that you are authorized to access.
-

Changing Your Password

Note

The *My Account* section can only be used to view and modify the details of the administrator that is currently logged in. The ability to change the administrator password is dependent on the configuration of the associated access profile setting (see *AccountMgt* under [Available Permission Groups / Access Profiles on page 471](#)).

To change your password:

Procedure

- Step 1** Browse to *My Account > Account Settings*.
- Step 2** Click the **Change Password** button.
- Step 3** Enter your existing password, and your new password, including confirmation.
- Step 4** Click the **Submit** button.
-

Your password is updated within the system.

To ensure that your password is secure, the system requires an alpha-numeric password that contains at least six characters. See [Keeping your system secure on page 27](#) for further information.

Creating a New super-user Account

Procedure

To add a new administration user:

- Step 1** Click the **Add** button at the top of the *User Management* screen. The *Add Administrator* screen is displayed.
- Step 2** Enter the user's details. The fields available in this section of the screen are to do with basic user information:

Field	Description	Remarks
Username	The id of the user.	<p>Must be unique across the platform, and is a mandatory field.</p> <p>Best Practice: Consider implementing a user name convention.</p> <p>Note: Once a user group has been configured for a customer, the usernames of all end-users added at the relevant customer are automatically combined with the user group to create a unique user name, for example username@usergroup; where the username (entered in this field) is displayed adjacent to the user group (already configured by the System, Provider or Reseller administrator).</p> <p>See also the <i>UsernameValidation</i> setting at Provider Preference and Settings on page 937</p>
Security profile	The security profile related to the customer.	This is an optional field. Options include security profiles that have been configured for your system as well as the None and Default options.
Password	Initial password for user login into the GUI.	This is a mandatory field.
Role	User role in the platform.	<p>This is an optional field, choose from drop-down list.</p> <p>User can only have one role. The user role defines what "type" of user they are and what sort of functions they can perform in the system.</p> <p>For example:</p> <p>Location Administrator</p> <p>Note: Administrators can only add a new administrator at a level lower than their own level in the administration hierarchy. Location administrators therefore do not have the option of adding a new administration user.</p>

Field	Description	Remarks
Web service access	Identifies the user's credentials for use by Web services API's, for example a 3rd Party system registering a phone.	This is an optional field. Checkbox selected = Enabled (Web service access allowed), Checkbox not selected = disabled (not allowed).
Title	Title of user.	-
First name	First Name of user.	-
Middle name	Middle name of user.	-
Last name	Last name (surname) of user.	This is a mandatory field. Sometimes referred to as "Surname".
Home telephone number	Home telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Mobile telephone number	Mobile telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Contact telephone number	Contact telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Alternative telephone number	Alternative telephone number for user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Email address	User email address.	This is not a mandatory field for end-user accounts, it is however useful to setup all users with their correct email addresses.
Job title	Job title of user.	-
Directory filter	Filter to be applied to the directory	-
Information	Additional Information for user.	-
Misc	-	-
Welcome message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-

Step 3 After completing the relevant fields on this page, click the **Next** button.

The fields available on the second page include:

Field	Description	Remarks
GUI Branding	The branding theme (colors, fonts, items look & feel etc.) to be presented to the user when they log in to the GUI.	Select from the drop-down list The branding themes are defined by the Provider administrator. The applicable branding themes should be enabled for each level in the hierarchy.

Field	Description	Remarks
Preferred country	Displays the preferred country.	Select from the drop-down list.
Access profile	Defines menu options available for the user.	This is a mandatory field. Select from the drop-down list. The available access profiles are defined by the Provider Administrator. Default access profile is provided as part of the product.
Account number to use in the external accounting system.	The account number to use in the external accounting system.	Enter the account number to use in the external accounting system.

Step 4 Complete the required fields and click the **Add** button. The user account is added to the system.

Note

When logging in for the first time, the new administration user is prompted to change their password.

Managing Your Administrator Account

Administrators manage their details, preferences and passwords via the *My Account* option on the main menu.

Note

- The *My Account* section of the system can only be used to view and modify the details of the administrator that is currently logged in.
- Only administrators can use this section to manage their details. End users must use the Self Care user interface to manage their details.

Procedure

Modifying your Details

To modify your details:

Step 1 Browse to *My Account > Account Settings*.

Step 2 Modify the required fields. The following fields are available:

Field	Remarks
Username	The username for the administrator.
First name	The administrator's first name.
Middle name	The administrator's middle name, if appropriate.
Last name	The administrator's last name. This is a mandatory field.
Email address	An email address for the administrator. This is not a mandatory field, but it is good practice to populate this field.
Ex directory	Select this checkbox to exclude the administrator from the corporate directory.
Preferred country	Select the preferred country for the administrator from the drop-down list.

Step 3 Click the **Modify** button. Your details are updated within the system.

Procedure

Changing your Password

Note

Users can change their own password.

To change your password:

- Step 1** Browse to *My Account > Account Settings*.
 - Step 2** Click the **Change Password** button.
 - Step 3** Enter your current password, your new password and confirmation of your new password.
 - Step 4** Click the **Submit** button when complete. Your password is updated.
-

Procedure

Changing your Preferences

To change your preferences:

- Step 1** Browse to *My Account > Account Settings*.
 - Step 2** Click the **Preferences** button.
 - Step 3** Select the required preference *Name* (active text link).
 - Step 4** Complete any required fields and then click the **Modify** button. The preference is applied to your user profile.
-

Configuring Resources

The purpose of this section is to describe the configuration of a range of resources that include base resources, a dial plan, a hardware set, providers, services, as well as a number of servers.

Setup of Base Resources

Base resources in the system are setup via the *Setup Tools* menu. The *Setup Tools* menu provides access to the following functionality:

- Global Settings
- Images
- Branding
- Themes
- Phone Types
- Button Groups
- Service Types
- Access Profiles
- Feature Display Policies
- Audit
- Bulk Load Samples
- About

- Security Profiles

Image Management

This screen is used to add (upload) images to the system by clicking the **Add** button. These images are typically used for selection as either as landing page or login images, such as company and corporate logos, or as customized branding images.

You can add images to one of two image groups, namely:

- Landing or Login Image Group
- Branding Image Group

You can also view an image group by selecting the required image group *name* (active text link).

Adding Images

Procedure

To add an image:

- Step 1** Browse to *Setup Tools > Images*.
- Step 2** Click the **Add** button.
- Step 3** Select the image to upload by clicking the **Choose File** button, and then browsing to and selecting the required image.
- Step 4** Select the group name in which to include the image from the drop-down list, or if you want to create a new image group, specify the name in the provided text field.
- Step 5** Select the required image group type from the drop-down list, available options are *Branding* or *Landing and Login*.
- Step 6** Click the **Upload File** button when complete.

The image is added to the system. The *Image Upload Status* screen is displayed summarizing the state of the requested image upload. When an image is uploaded successfully, a message is displayed stating, *Successfully uploaded image*. If the upload was not successful, an error message is displayed outlining the problem encountered.

Image Management

This screen is used to view all images in the selected image group (Landing/Login or Branding).

Add additional images to the image group by clicking the **Add** button.

Restore all images on the server by clicking the **Restore all Images on this server button**.

Manage an existing image by selecting the required image *Name* (active text link).

See also:

- [Adding Images on page 37](#)
- [Modifying or Deleting an Image on page 37](#)

Modifying or Deleting an Image

Procedure

Modifying an Image

To modify an image:

- Step 1** Browse to *Setup Tools > Images*.
- Step 2** Select the required image *Name* (active text link) from either the *Brand Image* or *Landing and Login Image Group* that you want to modify. The selected image is displayed on the *Manage Uploaded Images* screen.
- Note**
- Use the search functionality to locate the image if required.
- Step 3** Set the width and height of the image (maximum: W=300, H=150).
- Step 4** Set the required background colour, for example #FFFFFF = white (refer to any typical HTML color code chart for color values).
- Step 5** Select the required checkbox(es) to determine on which page(s) to display the image:
- Landing Page
 - Admin Login Page
 - Self Care Login Page
- Step 6** Click the **Submit** button when complete.

Procedure

Deleting an Image

To delete an image:

- Step 1** Browse to *Setup Tools > Images*.
- Step 2** Select the required image *Name* (active text link) from either the *Brand Image* or *Landing and Login Image Group* that you want to delete. The selected image is displayed on the *Manage Uploaded Images* screen.
- Note**
- Use the search functionality to locate the image if required.
- Step 3** **Note**
- The **Delete** button is only visible if the image is not being used anywhere in the system, that is all three checkboxes are empty (not selected).
- Click the **Delete** button. After confirming the deletion operation, the image is deleted from the system.
-

Phone Types

Verifying Phone Types/Expansion Module details

When adding a phone type or expansion module to the system, you are required to know the Cisco Product ID number (enum). If you would like to verify phone types and/or expansion module details, run the following SQL queries on the Cisco Unified Communications Manager (Unified CM):

Note

- These should work for all versions of Unified CM (4.2, 5.1, 6.1, 7.1.8 and up).
- SQL can be run against the Unified CM by logging onto the CLI and entering:

```
run sql <sql query>
```

- **For phones:**

```
select enum,name from typemodel where tkclass = 1
CCM DB Field = USM Field
enum = Product ID
name = Product Name
```

- **For expansion modules:**

```
select enum,name from typemodel where tkclass = 16
CCM DB Field = USM Field
name = Product Name
```

Phone Type Management

The system manages many types of IP phones and devices and each phone can have a number of unique characteristics. The *Phone Types* page enables each phone type to be created within the system.

Note

- The steps below are for adding phone types during or after initial deployment.
 - 69XX phones require UCM 7.1.3.32014 or later due to AXL bug CSCtc71858. An AXL API error about Network MoH not being available is returned when trying to add or update a 69XX phone. Unified CM 8.0 is not affected.
 - Blackberry phones are currently not supported by the system.
-

Note

- The system enables an administrator to specify which expansion modules (if any) can be associated to a specific phone type. Always ensure that the relevant expansion modules have been configured to allow the required phone types to use them.
 - Phone types can be added using bulk loaders. The sample system Base data bulk loader loads a set of common phone types. A list of phone types included in this sample loader can be found under [Phone Types on page 927](#). Only super users can add, delete or modify phone types.
 - The 3911, 3951, 6901 and 6911 phone types do not support extension mobility. To register these phones, the Allow user login to phone option in the phones' feature group must be disabled.
-

To view available Phone Types, browse to *Setup Tools > Phone Types*. A list of the available Phone types is displayed. This list includes the name of each Phone Type and a short description.

Adding a Phone Type

Provider administrators (or higher) can add new phone types to the Cisco Unified Communications Domain Manager (CUCDM) . This is typically required when new phone types are released, and subsequently added to the Cisco Unified Communications Manager (Unified CM).

Procedure

To add a new phone type:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the *Phone Type Management* active text link.
- Step 3** Click the **Add** button.
- Step 4** Complete all of the required fields and then click the **Add** button.

The phone type is added and appears in the phone menu within CUCDM.

Note

Phone type configuration must also be manually configured in the Unified CM. CUCDM is not able to automate this configuration as the AXL/SOAP interface to Unified CM does not allow these settings to be changed.

The following fields are available when adding a new phone type:

Field	Description
Field	Description
<i>Name</i>	Enter the name of the phone type being added. This is a mandatory field.
<i>Description</i>	Enter a short description of the phone type being added. This is a mandatory field.
<i>Product</i>	Enter the name of the product being added. This is a mandatory field.
<i>Product Model ID</i>	Enter the product model ID of the Phone type being added. This is a mandatory field.
<i>Protocol</i>	Select the protocol from the drop-down list that this phone type is using. Only phone types with a protocol supported by the system can be added to the system. This is a mandatory field.
<i>Hostname Prefix</i>	Enter the host name prefix for the Phone Type.
<i>Device Name Format</i>	<p>Enter the device name format for the Phone Type. This field is used to validate the device name when a new phone is added.</p> <p>Note</p> <p>In the case of the CUPC SIP and the iPhone phone types, the following should be the device name format: [0-9A-Z._-]{1,12}. This means that for these phone types a phone's name can be alphanumeric, with the special characters ".", "_", and "-" allowed; it can only be upper-case and must be a minimum length of 1 and a maximum length of 12.</p>
<i>Max. Number of Lines</i>	Select the maximum number of available lines from the drop-down list.
<i>Max. Number of SpeedDials</i>	Select the maximum number of available speed dials from the drop-down list.
<i>Max. Number of Busy Lamp Fields</i>	Select the maximum number of available busy lamp fields from the drop-down list.
<i>Max. Number of Service URLs</i>	Select the maximum number of service URLs for the phone type being added from the drop-down list.
<i>Max. Number of Softkeys</i>	Select the maximum number of available soft keys from the drop-down list.
<i>Max. Number of Buttons</i>	Select the maximum number of available button from the drop-down list.
<i>Screen Available (check for Yes)</i>	Select this checkbox if the phone type being added has a screen.

Field	Description
<i>Color screen (check for Yes)</i>	Select this checkbox if the phone type being added has a color screen.
<i>Max. Calls Waiting</i>	Select the maximum number of available calls waiting from the drop-down list.
<i>Default Max. Number of Calls Waiting</i>	Select the default maximum number of calls waiting from the drop-down list.
<i>Max. Busy Trigger Value</i>	Select the maximum busy trigger value from the drop-down list.
<i>Default Max. Busy Trigger Value</i>	Select the default busy trigger value from the drop-down list.
<i>Max. No Answer Ring Duration</i>	Select the maximum no answer ring duration. This value is entered in seconds
<i>Default Max. No Answer Ring Duration</i>	Select the default maximum no answer ring duration from the drop-down list. This value is entered in seconds.
<i>Expansion Module Capable</i>	<p>Select this checkbox if the phone type being added is Expansion Module Compatible and you would like this phone type to be able to use expansion modules. If expansion module support is disabled, the option to add expansion modules is not available when registering a phone of this particular type. If expansion module support is enabled and the number of expansion modules (provided below) has been specified, the number of expansion modules available is limited accordingly when registering that particular phone type.</p> <p>Note</p> <p>An administrator can specify which expansion modules (if any) can be associated to a specific phone type. Always ensure that the relevant expansion modules have been configured to allow the required phone types to use them.</p>
<i>Max Expansion Modules</i>	Specify the maximum number of expansion modules that can be added to this type of phone.
<i>Supports softkey templates (check for Yes)</i>	Select this checkbox if the phone type being added supports the use of softkey templates.
<i>MAC Address Required</i>	Select this checkbox if the phone type being added requires a MAC address.
<i>Dual Mode</i>	Select this checkbox if the phone type being added is a dual mode phone, for example Cisco Dual Mode for Android.
<i>Supports AAR</i>	Select this checkbox if the phone type being added supports AAR.
<i>Use Alternate Site CSS</i>	Select this checkbox if the phone type being added must use an alternate site CSS.
<i>Supports Recording</i>	Select this checkbox if the phone type being added supports recording.
<i>Supports IP Phone Services</i>	Select this checkbox if the phone type being added supports IP phone services.
<i>Owner Username Required</i>	Select this checkbox if the phone type being added must be associated to an end-user.
<i>Mobility User Required</i>	Select this checkbox if the phone type being added requires a mobility user.
<i>Supports Third Party Registration</i>	Select this checkbox if the phone type being added supports third party registration.

Field	Description
<i>Supports Call Barring</i>	Select this checkbox if the phone type being added supports the call barring feature.
<i>Device CSS Configurable</i>	Select this checkbox if the CSS for the phone type being added is configurable.
<i>Requires Phone Button Template</i>	Select this checkbox if the phone type being added must have a phone button template.
<i>Supports Extension Mobility</i>	Select this checkbox if the phone type being added supports extension mobility.

Modifying and Deleting a Phone Type

Procedure

To modify a Phone Type:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the **Phone Type Management** active text link.
- Step 3** Select the **Phone Type** (active text link) that you would like to modify.
- Step 4** Modify the fields (see [Adding a Phone Type on page 39](#)), and click the **Modify** button.

The Phone type is updated in the system.

Procedure

To delete a Phone Type:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the **Phone Type Management** active text link.
- Step 3** Select the **Phone Type** (active text link) that you would like to delete.
- Step 4** Click the **Delete** button.

After confirming the operation, the Phone type is deleted from the system.

Expansion Module Types

The system enables administrators to add expansion modules to the system.

Note

- The system enables an administrator to specify which expansion modules (if any) can be associated to a specific phone type. Always ensure that the relevant phone types are configured correctly to accept the relevant expansion modules.
- Expansion Module Types can also be added using bulk loaders. The sample system Base data bulk loader loads a set of common expansion modules. A list of expansion modules types included in this sample loader can be found under [Expansion Modules on page 931](#).

Expansion Module Management

Procedure

Managing Expansion Modules

Follow these steps to view available Expansion Module Types:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the **Expansion Module Type Management** active text link.

A list of the available Expansion Module Types is displayed. This list includes the name of each expansion module product name and a short description.

[Adding Expansion Module on page 43](#)

Procedure***Modify Expansion Modules***

To modify Expansion Modules:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the *Expansion Module Management Types* active text link.
- Step 3** Select the *Expansion Modules* (active text link) that you would like to modify.
- Step 4** Modify the required fields and click the **Modify** button.

The Expansion Module Type is updated in the system.

Procedure***Delete Expansion Modules***

To delete an Expansion Module Type:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the *Expansion Module Management Types* active text link.
- Step 3** Select the *Expansion Modules* (active text link) that you would like to delete.
- Step 4** Click the **Delete** button.

After confirming the operation, the Expansion Module type is deleted from the system.

Adding Expansion Module**Procedure*****Adding Expansion Module Types***

To add a new Expansion Module type:

- Step 1** Browse to *Setup Tools > Phone Types*.
- Step 2** Select the *Expansion Module Type Management* active text link.
- Step 3** Click the **Add** button.
- Step 4** Complete all of the required fields and then click the **Add** button.

The Expansion Module Type is added to the system.

The following fields are available when adding a new Expansion Module Type:

Field	Description
<i>Name</i>	Enter the name of the Expansion Modules being added. This is a mandatory field.
<i>Expansion Module Product Name</i>	Specify the Expansion Module Product Name being added. This is a mandatory field.
<i>Max. Lines Supported</i>	Select the maximum number of available lines from the drop-down list. This is a mandatory field.

Service Types

The system manages many types of IP services and classes of services. Each service needs to be clearly defined within the system to assist with identifying drivers and ensuring the trouble free delivery of the services. Service types often require that multiple systems work together. Quite often it may appear that the system is performing no action on the specific service, however, the system plays an important co-ordination role, and enables multiple systems to work seamlessly together to provide a service.

Procedure

Searching Service Types

To search for a service type:

- Step 1** Browse to Setup Tools > Services Type.
- Step 2** Select the search criteria from the *Search by* drop-down list, then enter the relevant key words for the search in the text-box adjacent to the *Max results* drop-down list.
- Step 3** Click the **Search** button.

The search results are displayed

Available fields include:

Field	Description
<i>Search by</i>	The search can be based on <i>Service Name</i> , <i>Description</i> or <i>Service Category</i> , selected from the drop-down list.
<i>Max results</i>	The maximum number of search results to display, selected from the drop-down list.

Adding a Service Type

Procedure

To add a service type to the system:

- Step 1** Browse to *Setup Tools > Services Type*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields and click the **Add** button.

The service type is added to the system, and appears in the services and feature group menus.

The following fields are available when adding a service type:

Field	Description
<i>Service Name</i>	The name of the service. This is a mandatory field.

Field	Description
<i>Description</i>	A short description of the Service Type being added. This is a mandatory field.
<i>Number of Lines</i>	Only required for Service Categories inward calls & line
<i>Tag</i>	The Service tag is critical as it provides the link to other systems that must also support the Services, such as Call Manager and the relevant Dial Plan. This is a mandatory field.
<i>Service Category</i>	Select the required Service Category from the drop-down list. This is a mandatory field. Note The <i>phoneapplication</i> category is no longer valid and should not be selected.
<i>URL</i>	Specify the URL related to the Service Type.
<i>Idle Timeout</i>	Specify the idle time out period, in seconds, for the Service Type.
<i>Self Care</i>	Select this checkbox if you this service type is going to be used by Self-care.

Note

- In many cases, adding the service to the system and to the dial plan results in all the other systems being configured automatically.
- In certain cases, manual configuration of some systems is still required.
- When creating a Voicemail Service Template(User Template) in Cisco Unity Connection Server, the template name may not include parenthesis "()". The Rest API that is used to import the templates do not support "(" in the template name.

See also: [Viewing, Modifying and Deleting Service Types on page 45](#)

Viewing, Modifying and Deleting Service Types

Procedure

To view and modify a service type:

- Step 1** Browse to *Setup Tools > Services Type*.
- Step 2** Select the *Service Type* (active text link) that you would like to view/modify.
- Step 3** Make the required modifications and click the **Modify** button.

The service type is updated within the system.

Procedure

Deleting a Service Type

To delete a service type:

- Step 1** Browse to *Setup Tools > Services Type*.
- Step 2** Select the *Service Type* (active text link) that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the service type is deleted.

Country Management

Within the system, countries are managed at two levels, the provider level and the global (system) level. Hence, countries are managed in two respective sections, the *Provider Administration* menu and the *Dial Plan* menu.

Overview of managing countries:

- The Dial Plan menu is used to manage countries at a global level.

Note

Providers are only able to add countries that have already been added via the Dial Plan menu - see: [Dial-plan Countries on page 48](#).

- The Provider Administration menu is used to manage countries at a provider level - see: [Provider Country Management on page 675](#).

View and Modify a Country

Providers are able to operate in a multi-country environment. Each country however, has unique dial plan elements and number configurations, so the system needs to apply these different configurations to each location based on the country they are allocated.

Procedure

View and Modify Countries

To view and modify a country:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
 - Step 2** Select the Country *Name* (active text link) of the country that you would like to view.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The relevant details of the selected country are updated in the system.

The following fields are available while modifying a country:

Fields	Description
Country	Select the name of the country that you would like to add from the drop-down list. This is a mandatory field.
ISO Country Code	You do not need to specify this field, the system will complete this field for you.
International Dial Code	Specify the international dial code for the country being added. For example, the UK would be 44. This is a mandatory field.
International Access Prefix	This is the code used to dial out of the country being added (i.e. for a call to Spain or France). For example, in the UK this would be 00. This is a mandatory field.
Standard Access Prefix	The prefix used when making a standard phone call within the country (i.e. for a call to your neighbor). For example, in the UK this would be 0.
Premium Access Prefix	The prefix used when making a premium call within the country (i.e. for a call to an information service such as weather or news service). For example, in the UK this would be 9.

Fields	Description
Emergency Access Prefix	The prefix used when making an emergency call within the country (i.e. for a call to the fire department/service). For example, in the UK this would be 999. This is a mandatory field.
Service Access Prefix	The prefix used when making a service call within the country (i.e. for a call to your telephone service provider). For example, in the UK this would be 111.
CLI On Prefix	The prefix used within the country when CLI is active.
National Trunk Prefix	The National Trunk Prefix used within the country. For example, in the UK this would be 0.
PSTN Access Prefix	The PSTN Access Prefix used within the country. For example, in the UK this would be 9.
Default User Locale	The Default User Locale is used when phones or mobility profiles are bulk loaded, with the phone locale set to "auto". If set to "auto", then the default user locale for the country of the location where the phone or extension mobility profile resides in, is used. The default user locale is also used with the migration from the old phone locale (ISO country code) when the phone locale for a phone or mobility profile is set to "auto". In this case, the same selection method as describe above is used.
Network Locale	Enter the required Unified CM network locale name to be used by phones in the specified country. This contains a definition of the tones and cadences that the phones will use.
Full National Number Rules	This section is used to configure the national number rules. Available options include enforcing E164 rules, maximum area code length, minimum area code length, maximum local number length and minimum local number length.
Non-Geographic E164 Emergency CLI Preference for Local Gateway Breakout	This section is used to configure non-geographic E164 emergency CLI preference for local gateway breakout. Here you are able to specify whether the Local Gateway CLI Preference is based on a Device CLI or Published Number.
Non-Geographic E164 Emergency CLI Preference for Central Gateway Breakout	This section is used to configure the non-geographic E164 emergency CLI preference for central gateway breakout. Here you are able to specify whether the Central Gateway CLI Preference is based on a Device CLI or Published Number.
Supported Gateway Call Routing Types	This section is used to manage the supported gateway call routing types for the selected country. Here you are able to modify the country call type names and associate particular call types with countries. Select the checkboxes adjacent to the call types that you would like to associate with the country. To edit the name of a call type, edit the name in the provided text box, then click the Modify button. Note: If this has been configured at the location level, you can modify the name but not the call types association to a country.

Procedure

Delete a Country

To delete a country from the system:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Delete** button adjacent to the country that you would like to delete.

After confirming the deletion operation, the country is deleted from the system.

Dial-plan Countries

Procedure

View and Modify Countries

To view and modify a country:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Select the *Country Name* (active text link) of the country that you would like to view.
- Step 3** Modify the required fields and click the **Modify** button.

The relevant details of the selected country are updated within the system.

Procedure

Add a Country

To add a country at the system level in the system:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Add** button.
- Step 3** Provide all of the required details. The following fields are available when adding a country to the system:

Field	Description	Remarks
Country	Select the name of the country that you would like to add from the drop-down list.	This is a mandatory field.
International Dial Code	Specify the international dial code for the country being added.	This is a mandatory field. For example, the UK would be 44.
International Access Prefix	This is the code used to dial out of the country being added (i.e. for a call to Spain or France).	This is a mandatory field. For example, in the UK this would be 00.
Standard Access Prefix	The prefix used when making a standard phone call within the country (i.e. for a call to your neighbor).	For example, in the UK this would be 0.
Premium Access Prefix	The prefix used when making a premium call within the country (i.e. for a call to an information service such as weather or news service).	For example, in the UK this would be 9.
Emergency Access Prefix	The prefix used when making an emergency call within the country (i.e. for a call to the fire department/service).	This is a mandatory field. For example, in the UK this would be 999.
Service Access Prefix	The prefix used when making a service call within the country (i.e. for a call to your telephone service provider).	For example, in the UK this would be 111.

Field	Description	Remarks
CLI On Prefix	The prefix used within the country when CLI is active.	
National Trunk Prefix	The National Trunk Prefix used within the country.	For example, in the UK this would be 0.
PSTN Access Prefix	The PSTN Access Prefix used within the country.	For example, in the UK this would be 9.
Default User Locale	Enter the country name.	The Default User Locale is used when phones or mobility profiles are bulk loaded, with the phone locale set to "auto". If set to "auto", then the default user locale for the country of the location where the phone or extension mobility profile resides in, is used. The default user locale is also used with the migration from the old phone locale (ISO country code) when the phone locale for a phone or mobility profile is set to "auto". In this case, the same selection method as describe above is used.
Network Locale	Enter the required network locale name.	This contains a definition of the tones and cadences that the phones in the specified user locale will use.
Full National Number Rules	This section is used to configure the national number rules.	Available options include enforcing E164 rules, maximum area code length, minimum area code length, maximum local number length and minimum local number length.
Non-Geographic E164 Emergency CLI Preference for Local Gateway Breakout	This section is used to configure non-geographic E164 emergency CLI preference for local gateway breakout.	Here you are able to specify whether the Local Gateway CLI Preference is based on a Device CLI or Published Number.
Non-Geographic E164 Emergency CLI Preference for Central Gateway Breakout	This section is used to configure the non-geographic E164 emergency CLI preference for central gateway breakout.	Here you are able to specify whether the Central Gateway CLI Preference is based on a Device CLI or Published Number.
Supported Gateway Call Routing Types	This section is used to manage the supported gateway call routing types for the selected country. Here you are able to modify the country call type names and associate particular call types with countries.	<p>Select the checkboxes adjacent to the call types that you would like to associate with the country. To edit the name of a call type, edit the name in the provided text box, then click the Modify button.</p> <p>Note</p> <p>If this has been configured at the location level, you can modify the name but not a call types association to a country.</p>

Step 4

Click the **Add** button. The country is added to the system and appears in all of the relevant drop-down menus for resources and number configuration.

Procedure

Delete a Country

To delete a country from the system:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Delete** button adjacent to the country that you would like to delete.
-

After confirming the deletion operation, the country is deleted from the system.

Country Management within a Provider**Procedure**

View countries within a Provider

To view a country:

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Select the *Country Name* (active text link) of the country that you would like to view. The system displays the relevant details of the selected country. The following fields are available when viewing a country at the provider level:

Field	Description
Country	The name of the country being viewed. For example, "United Kingdom".
ISO Country Code	The ISO code for the country being viewed, the system completes this field for you when adding a country. For example, for the United Kingdom, the ISO code displayed is "GBR".

Procedure

Add a Country to a provider

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Click the **Add** button.
- Step 3** Select the relevant Country from the drop-down list and click the **Add** button.
-

The Country is added to the provider within the system.

Procedure

Delete a Country

To delete a country from a provider:

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Click the **Delete** button adjacent to the country that you would like to delete.

After confirming the deletion operation, the country is deleted from the system.

Adding a Country

Providers are able to operate in a multi-country environment. Each country however, has unique dial plan elements and number configurations, so the system needs to apply these different configurations to each location based on the country they are allocated. Hence, countries can be managed from two sections within the system, the *Dial Plan* menu and from the *Provider Administration* menu.

Overview of Managing Countries:

- The *Dial Plan* menu is used to manage countries at a global level, providers are only able to add countries that have already been added via the *Dial Plan* menu. For instructions on adding countries within the system, see the *Add* section below.
- The *Provider Administration* menu is used to manage countries at a provider level, providers are only able to add and modify countries that have been added via the *Dial Plan* menu. For instructions on adding a country at the provider level, see the *Provider - Countries* section.

Procedure

Add a Country to the System

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Add** button.
- Step 3** Provide all of the required details and click the **Add** button.

The Country is added to the system and appears in all of the relevant drop-down menus for resources and number configuration.

The following fields are available when adding a country to the system:

Fields	Description
Country	Select the name of the country that you would like to add from the drop-down list. This is a mandatory field.
ISO Country Code	You do not need to specify this field, the system will complete this field for you.
International Dial Code	Specify the international dial code for the country being added. For example, the UK would be 44. This is a mandatory field.
International Access Prefix	This is the code used to dial out of the country being added (i.e. for a call to Spain or France). For example, in the UK this would be 00. This is a mandatory field.
Standard Access Prefix	The prefix used when making a standard phone call within the country (i.e. for a call to your neighbor). For example, in the UK this would be 0.
Premium Access Prefix	The prefix used when making a premium call within the country (i.e. for a call to an information service such as weather or news service). For example, in the UK this would be 9.
Emergency Access Prefix	The prefix used when making an emergency call within the country (i.e. for a call to the fire department/service). For example, in the UK this would be 999. This is a mandatory field.

Fields	Description
Service Access Prefix	The prefix used when making a service call within the country (i.e. for a call to your telephone service provider). For example, in the UK this would be 111.
CLI On Prefix	The prefix used within the country when CLI is active.
National Trunk Prefix	The National Trunk Prefix used within the country. For example, in the UK this would be 0.
PSTN Access Prefix	The PSTN Access Prefix used within the country. For example, in the UK this would be 9.
Default User Locale	The Default User Locale is used when phones or mobility profiles are bulk loaded, with the phone locale set to "auto". If set to "auto", then the default user locale for the country of the location where the phone or extension mobility profile resides in, is used. The default user locale is also used with the migration from the old phone locale (ISO country code) when the phone locale for a phone or mobility profile is set to "auto". In this case, the same selection method as describe above is used.
Network Locale	Enter the required Unified CM network locale name to be used by phones in the specified country. This contains a definition of the tones and cadences that the phones will use.
Full National Number Rules	This section is used to configure the national number rules. Available options include enforcing E164 rules, maximum area code length, minimum area code length, maximum local number length and minimum local number length.
Non-Geographic E164 Emergency CLI Preference for Local Gateway Breakout	This section is used to configure non-geographic E164 emergency CLI preference for local gateway breakout. Here you are able to specify whether the Local Gateway CLI Preference is based on a Device CLI or Published Number.
Non-Geographic E164 Emergency CLI Preference for Central Gateway Breakout	This section is used to configure the non-geographic E164 emergency CLI preference for central gateway breakout. Here you are able to specify whether the Central Gateway CLI Preference is based on a Device CLI or Published Number.
Supported Gateway Call Routing Types	This section is used to manage the supported gateway call routing types for the selected country. Here you are able to modify the country call type names and associate particular call types with countries. Select the checkboxes adjacent to the call types that you would like to associate with the country. To edit the name of a call type, edit the name in the provided text box, then click the Modify button. Note: If this has been configured at the location level, you will be able to can modify the name but not the call types association to a country.

Dial-plan Countries

Procedure

View and Modify Countries

To view and modify a country:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Select the Country *name* (active text link) of the country that you would like to view.
- Step 3** Modify the required fields and click the **Modify** button.

The relevant details of the selected country are updated within the system.

Procedure

Follow the steps below to add a country at the system level in the system:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Add** button.
- Step 3** Provide all of the required details. The following fields are available when adding a country to the system:

Country	Select the name of the country that you would like to add from the drop-down list.	This is a mandatory field.
International Dial Code	Specify the international dial code for the country being added.	This is a mandatory field. For example, the UK would be 44.
International Access Prefix	This is the code used to dial out of the country being added (i.e. for a call to Spain or France).	This is a mandatory field. For example, in the UK this would be 00.
Standard Access Prefix	The prefix used when making a standard phone call within the country (i.e. for a call to your neighbor).	For example, in the UK this would be 0.
Premium Access Prefix	The prefix used when making a premium call within the country (i.e. for a call to an information service such as weather or news service).	For example, in the UK this would be 9.
Emergency Access Prefix	The prefix used when making an emergency call within the country (i.e. for a call to the fire department/service).	This is a mandatory field. For example, in the UK this would be 999.
Service Access Prefix	The prefix used when making a service call within the country (i.e. for a call to your telephone service provider).	For example, in the UK this would be 111.
CLI On Prefix	The prefix used within the country when CLI is active.	
National Trunk Prefix	The National Trunk Prefix used within the country.	For example, in the UK this would be 0.
PSTN Access Prefix	The PSTN Access Prefix used within the country.	For example, in the UK this would be 9.
Full National Number Rules	This section is used to configure the national number rules.	Available options include enforcing E164 rules, maximum area code length, minimum area code length, maximum local number length and minimum local number length.
Non-Geographic E164 Emergency CLI Preference for Local Gateway Breakout	This section is used to configure non-geographic E164 emergency CLI preference for local gateway breakout.	Here you are able to specify whether the Local Gateway CLI Preference is based on a Device CLI or Published Number.

Country	Select the name of the country that you would like to add from the drop-down list.	This is a mandatory field.
Non-Geographic E164 Emergency CLI Preference for Central Gateway Breakout	This section is used to configure the non-geographic E164 emergency CLI preference for central gateway breakout.	Here you are able to specify whether the Central Gateway CLI Preference is based on a Device CLI or Published Number.
Supported Gateway Call Routing Types	This section is used to manage the supported gateway call routing types for the selected country. Here you are able to modify the country call type names and associate particular call types with countries.	<p>Select the checkboxes adjacent to the call types that you would like to associate with the country. To edit the name of a call type, edit the name in the provided text box, then click the Modify button.</p> <p>Note</p> <p>If this has been configured at the location level, you will be able to modify the name but not a call types association to a country.</p>

- Step 4** Click the **Add** button. The country is added to the system and appears in all of the relevant drop-down menus for resources and number configuration.

Procedure

To delete a country from the system:

- Step 1** Select the *Countries* tab in the *Dial Plan Tools* menu.
- Step 2** Click the **Delete** button adjacent to the country that you would like to delete.
-

After confirming the deletion operation, the country is deleted from the system.

Dial Plan Tools Overview

The *Dial Plan Tools* menu provides access to the following functionality:

- Number Construction
- Hardware Sets
- Configuration Models
- Countries
- Model Management
- Migrate Models

Dial Plan Management

Number Construction involves the configuration of variables such as:

- Codec settings (compression and decompression standards)
- Site number formats
- Site display formats
- Multi-tenant capabilities
- Dial prefixes
- Number formats

Number Construction also allows for the definition of Published number formats via a Preferences setting.

Note

Number Construction can be Bulk Loaded, this reduces the risk of error and can be more efficient when uploading large data sets.

In each case, a different dial plan can be associated depending on the scenario, such as:

- Multi-Tenant
- Large Enterprise
- Branch Banking
- Business Park

For example, the Multi-tenant Dial plan must be associated with the PGW/CCM Hardware set, but other variants can have many permutations and combinations.

The CCM model management section provides the model loader programs (similar to Bulk Loaders), as well as a number of sample templates.

Each Model Loader is designed specifically for each relevant component in the iBVS platform, including:

- PGW
- Call Manager
- Gateways
- Application services, such as Voicemail

In the system, Dial Plans are managed mainly via the *Number Construction* option under the *Dial Plan Tools* menu.

Adding a Dial Plan

To add a Dial plan:

Procedure

- Step 1** Browse to *Dial Plan Tools > Number Construction*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields, and click the **Add** button. The dial plan is added to the system.

The following fields are available:

Fields	Description
Details	
Dial plan name	The name of the dial plan being added. This is a mandatory field.
Description	A short description of the dial plan being added.
Codecs	
Customer / Building Codec Configurable?	Select the Customer/Building Codec Configurable? checkbox if you would like customers/buildings to be able to select their own codecs.
Intra-Region Max Audio Bit Rate	This is the intra-region codec used by the system when setting up the per location Unified CM regions for locations. Select the required codec from the drop-down list.
Inter-Region Max Audio Bit Rate	This is the inter-region codec used by the system when setting up the per location Unified CM regions for locations. Select the required codec from the drop-down list.
Dial Plan Rules	
Multi-Tenant Dial Plan?	This checkbox determines whether or not this is a Multi-Tenant Dial Plan. For the majority of dial plans, this setting is enabled. However, please check with your dedicated system support person when utilizing this feature.
Enforce HCS Dial Plan?	<p>This setting determines the behavior in a few places in the code which allows the flexibility of working around certain validations put in place for HCS. They are currently:</p> <ul style="list-style-type: none"> When a customer is created, PGW and TimesTen drivers perform no actions. When enabled, the requirement for the hardware group from addCustomer is removed, this enables the assignment of hardware groups to customer after they are created. Since there is no hardware for Add-Customer, there are no hardware transactions. When this option is selected, customers are able to access the <i>Customer Call Planner Management</i> screen by browsing to <i>General Administration > Customers > <Customer Name> > Advanced Mgt. > Call Planner Association</i>. This screen enables customers to associate and disassociate call planners (hardware groups).
Site Type Selection	
Site Type Support	This checkbox enables you to turn on support for site types, then select the site types you need below. These site types are selected when you add a location and the site type is appended to the end of model names for location transactions (e.g. <i>RegisterPhone-Office</i>).
Branch	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Branch.
Office	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is an Office.
Business	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Business.
Residential	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Residence.

Fields	Description
Internal Number Format This section is used to determine the format of the internal numbers (fints) in the system and their length. The fint currently needs to be unique in the system, so for example if you only tick 'include Site Code' then you cannot have the same site code in more than 1 customer (as the fint would be SiteCode + Extension only).	
Internal Number Component Order	Used to specify the order of number components. This field cannot be edited and is included for information purposes only. For example <i>CPID:RID:CID:SITECODE:EXTNNUMBER</i> .
Maximum Allowed Internal Number Length	This is the maximum allowed fint length. Default is 20 characters. This cannot be less than the total allocated digits and the internal fint digit length cannot be greater than the max allowed length. This is a mandatory field.
Includes CPID?	Select this checkbox if you would like the CPID to be included in the fint. Regardless of whether you select this option or not, CPIDs are still assigned to most devices, including PBXs, Transits, Gateways, Voice-mail, etc.
CPID Digits	The number of digits to use for the CPID. As the CPID is still allocated for hardware even if it's not being used in the fint, this should be set to a sensible number depending on the number of hardware devices being planned (i.e. at least 2 digits).
Includes RID?	Select this checkbox if you want the RID to be included in the fint. Regardless of whether you select this or not, RIDs are still allocated to Locations/Customers.
RID Digits	The number of digits to use for the RID. As RIDs are still allocated to locations even if it's not being used in the fint, this should be set to a sensible number depending on the number of locations/customers being planned (i.e. at least 3 digits).
Includes CID	Select this checkbox if you want the CID to be included in the fint. Regardless of whether you select this or not, CIDs are still allocated to Unified CM PBX clusters.
CID Digits	The number of digits to use for the CID. As CIDs are still allocated to Unified CM PBXs even if it's not being used in the fint, this should be set to a sensible number depending on the number of clusters being planned.
Includes Site Code?	Select this checkbox to include the site code in the fint. Regardless of whether you select this or not, Site Codes are still required for locations to be added.
Max. Site Code Digits	This number reflects the maximum number length of the site code.
Site Code Rules	Free text which is displayed next to site codes when they are being added to the system to communicate the rules imposed by the dial plan. This should be useful to the user, for example, <i>Maximum length of 4 digits</i> .

Fields	Description
Variable Length Internal Number?	Select this checkbox if you want the length of the extension portion of the fnt to be configurable. If <i>Variable Length Internal Number</i> is set to <i>Y</i> , the <i>Internal Number Length</i> field must be blank. Enabling this option results in an extension length setting being available during add location. This can be used to define the length of the extension. If this is not selected, the length of the extension is determined by taking the setting below and subtracting any other digits from it (i.e. a location has a site code of 123 (3 digits) and the dial plan calls for no CPID, no RID, and 7 for internal number length. This would result in the extension length being $4 = 7 - 3$.
Internal Number Length	This option enables the user to define the length of the internal number. This is used only if the variable length extension is not enabled. See the entry above to determine the extension length. This is a mandatory field.
Internal Number Display Rules These setting determine how internal numbers are displayed within the application. This drives a value, <code>displayfntnumber</code> , which is used anytime the fnt would be displayed to the user (within the GUI, Self Care, default line text in Unified CM, etc). Note If you change these settings, it does not affect any fnts already in the system. However, it does affect any new fnts added to the system (i.e. locations).	
Includes CPID?	Selecting this checkbox includes the CPID in the number display.
Includes RID?	Selecting this checkbox includes the RID in the number display.
Includes Site Code?	Selecting this checkbox includes the Site Code in the number display.
RID Type Selection	
Routing Identifier (RID)	Use the drop-down list to determine the hierarchy the RID is allocated at. The <i>Location</i> option, is currently the most common choice here.
Dial Prefixes This section covers any dial prefixes that are required for various call types. This allows the requirements to be turned on/off as well as specification of the value.	
Inter-Site Prefix Required?	Select this checkbox if an inter site prefix is required for the dial plan.
Inter-Site Prefix Configurable?	Select this checkbox if the prefix is a configurable value. This is configurable per customer and can be defined for the customer when adding. If not selected then the value used during the Add Customer operation will be hard coded.
PSTN Access Prefix Required?	Select this checkbox if a PSTN breakout code is required.
PSTN Access Prefix Configurable?	Select this checkbox if the prefix is a configurable value. This is configurable per location and can be defined for the location when adding. If not selected then the value used during the Add Location operation is hard coded.

Fields	Description
Call Park Prefix	<p>To distinguish between Call Park numbers internally, the system uses a custom prefix, followed by a number increment, one per call processing server in a Location's Unified CM cluster.</p> <p>The Prefix can be set by the system administrator, either at the System level, where it applies to all Locations (as a default,) or at the individual Location level. It can contain the characters #,* or 0-9, and the existing dial plan should be taken into consideration when assigning it.</p> <p>Because the Prefix is common to all Call Park internal numbers in a Location, the system uses a Sequence Number to ensure that all Call Park numbers are unique in a cluster. Call Park numbers are only created on Unified CM servers marked as Call Processor Engines (CPEs.) For each additional CPE that is targeted during the Call Park create sequence, the Internal Sequence Number portion of the Call Park identifier is incremented by one.</p> <p>Note</p> <p>To manage mega-clusters, which can handle up to 16 subscribers, the sequence number consists of two (2) digits. The sequence numbers range from 01 (for the first server) to 16 for the highest number of servers.</p> <p>For example, if an administrator selects #2 as a Call Park Prefix and creates a 10 number Call Park range, the numbers would be #20100, #20101 etc. on Server A and #20200, #20201 etc. on Server B.</p>
Call Park Location Configurable?	Select this checkbox if the prefix is a configurable value. If selected , the value in the Call Park Prefix field is displayed at a location level in a read-only text field. This is configurable per location and can be defined for the location when adding. If not selected , then the value used during the Add Location operation is hard coded.
Format of External Phone Number Mask on Unified CM <p>This section determines how external (E164/FNN) numbers are displayed in the system. This includes in drop-downs for assigning lines to phones/users and also for configuring the external mask in Unified CM for the lines.</p> <p>Note</p> <p>If you change this setting, it will not affect any FNNs already in the system. The displayed E164 value is determined for the number when it is added to the E164 inventory. It will affect any new FNNs added to the system.</p>	
Show PSTN Dial Prefix	This setting enables the inclusion of the PSTN breakout prefix on the front of the number.
Show Country Code	This setting enables the inclusion of the country code at the beginning of the number (e.g. 44 for the UK).
PSTN Access Prefix Configurable?	Select this checkbox if you would like the PSTN access prefix to be configurable.
Show National Code Prefix	This setting enables the display of the trunk access code on the front of the PSTN number (e.g. 0 for the UK).
Show National Code	This setting enables the display of the area code on the front of the PSTN number.

Fields	Description
Prefix Plus Symbol	This setting enables the inclusion of the international escape character at the beginning of the number.
Format of IPPBX Configured Internal Number This section determines how the FINT numbers are provisioned in the IPPBX system (the DN in Unified CM). This is generally done when you setup a device with an extension number (phones, user extension mobility, CTI, etc). This also affects any features that make use of the FINTs (e.g. Pickup Groups, Hunt Groups, SNR, etc). By default the settings for the <i>Includes SiteCode</i> and <i>Includes Extension</i> checkboxes are selected . Note If you change this setting, it does not affect any FINTs already provisioned in the system. It only affects any new FINTs added to the system. Changes can however be applied to existing locations using the iFint Migrate feature (see the Deployment Guide for more details on this tool). The full list of features that use the iFint logic are: <ul style="list-style-type: none"> • Phone Lines configuration • Extension Mobility Profile (Device Profile) lines • CTI route points - port lines • Analog Port Lines • Pick up Groups - number and members • Number Group (line group in Unified CM) members • Hunt Group Pilot numbers • Location Call Park Numbers • SNR Setup (Remote Destinations, etc) 	
Includes CID	Select this checkbox to include the CID in the external phone number mask.
Includes CPID	Select this checkbox to include the CPID in the external phone number mask.
Includes RID	Select this checkbox to include the RID in the external phone number mask.
Includes SiteCode	Select this checkbox to include the site code in the external phone number mask.
Includes Extension	Select this checkbox to include extensions in the external phone number mask.

Fields	Description
Format of Voicemail Configured Pilot Number This section determines how the Voicemail pilot numbers are provisioned in the IPPBX system (the DN in Unified CMr). The default setting for the <i>Includes Inter-site Prefix</i> checkbox is not selected (OFF) . The default setting for both the <i>Includes SiteCode</i> and the <i>Includes Extension</i> checkboxes is selected (ON) . Note These default settings are critical to ensure backward compatibility when a customer upgrades to a later software version. If you change these default settings, the Voicemail feature for your location will not function. Note Customers that are using only the extension number in their existing system configuration must unselect (switch off) the <i>Includes SiteCode</i> checkbox after performing an upgrade.	
Includes Inter-Site Prefix	Select this checkbox to include the inter-site prefix in the Voicemail pilot number.
Includes SiteCode	Select this checkbox to include the site code in the Voicemail pilot number.
Includes Extension	Select this checkbox to include the extension in the Voicemail pilot number.
Format of Voicemail Configured Mailbox Number This section determines how Voicemail mailbox numbers are provisioned in the IPPBX system (the DN in CallManager). The default setting for both the <i>Includes SiteCode</i> and the <i>Includes Extension</i> checkboxes is selected (ON) . Note These default settings are critical to ensure backward compatibility when a customer upgrades to a later software version. If you change these settings, the Voicemail feature for your location will not function. Note Customers that are using only the extension number in their existing system configuration must unselect (switch off) the <i>Includes SiteCode</i> checkbox after performing an upgrade.	
Includes SiteCode	Select this checkbox to include the site code in the Voicemail mailbox number.
Includes Extension	Select this checkbox to include the extension in the Voicemail mailbox number.

Viewing and Modifying a Dial Plan

Dial Plans are managed mainly via the *Number Construction* option under *Dial Plan Tools* menu.

Procedure

Modifying Dial Plans

To Modify a Dial Plan:

- Step 1** Browse to *Dial Plan Tools > Number Construction*.

- Step 2** Select the *Name* (active text link) of the Dial plan that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button. The dial plan is updated within the system.

The following fields are available when modifying the Dial Plan:

Fields	Description
Details	
Dial plan name	The name of the dial plan being added. This is a mandatory field.
Description	A short description of the dial plan being added.
Codecs	
Customer / Building Codec Configurable?	Select the Customer/Building Codec Configurable? checkbox if you would like customers/buildings to be able to select their own codecs.
Intra-Region Max Audio Bit Rate	This is the intra-region codec used by the system when setting up the per location Unified CM regions for locations. Select the required codec from the drop-down list.
Inter-Region Max Audio Bit Rate	This is the inter-region codec used by the system when setting up the per location Unified CM regions for locations. Select the required codec from the drop-down list.
Dial Plan Rules	
Multi-Tenant Dial Plan?	This checkbox determines whether or not this is a Multi-Tenant Dial Plan. For the majority of dial plans, this setting is enabled. However, please check with your dedicated system support person when utilizing this feature.
Enforce HCS Dial Plan?	<p>This setting determines the behavior in a few places in the code which allows the flexibility of working around certain validations put in place for HCS. They are currently:</p> <ul style="list-style-type: none"> When a customer is created, PGW and TimesTen drivers perform no actions. When enabled, the requirement for the hardware group from addCustomer is removed, this enables the assignment of hardware groups to customer after they are created. Since there is no hardware for Add-Customer, there are no hardware transactions. When this option is selected, customers are able to access the <i>Customer Call Planner Management</i> screen by browsing to <i>General Administration > Customers > <Customer Name> > Advanced Mgt. > Call Planner Association</i>. This screen enables customers to associate and disassociate call planners (hardware groups).
Site Type Selection	
Site Type Support	This checkbox enables you to turn on support for site types, then select the site types you need below. These site types are selected when you add a location and the site type is appended to the end of model names for location transactions (e.g. <i>RegisterPhone-Office</i>).
Branch	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Branch.
Office	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is an Office.
Business	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Business.

Fields	Description
Residential	If you have selected the <i>Site Type Support</i> option above, select this checkbox if your site is a Residence.
Internal Number Format This section is used to determine the format of the internal numbers (fints) in the system and their length. The fint currently needs to be unique in the system, so for example if you only tick 'include Site Code' then you cannot have the same site code in more than 1 customer (as the fint would be SiteCode + Extension only).	
Internal Number Component Order	Used to specify the order of number components. This field cannot be edited and is included for information purposes only. For example <i>CPID:RID:CID:SITECODE:EXTNNUMBER</i> .
Maximum Allowed Internal Number Length	This is the maximum allowed fint length. Default is 20 characters. This cannot be less than the total allocated digits and the internal fint digit length cannot be greater than the max allowed length. This is a mandatory field.
Includes CPID?	Select this checkbox if you would like the CPID to be included in the fint. Regardless of whether you select this option or not, CPIDs are still assigned to most devices, including PBXs, Transits, Gateways, Voice-mail, etc.
CPID Digits	The number of digits to use for the CPID. As the CPID is still allocated for hardware even if it's not being used in the fint, this should be set to a sensible number depending on the number of hardware devices being planned (i.e. at least 2 digits).
Includes RID?	Select this checkbox if you want the RID to be included in the fint. Regardless of whether you select this or not, RIDs are still allocated to Locations/Customers.
RID Digits	The number of digits to use for the RID. As RIDs are still allocated to locations even if it's not being used in the fint, this should be set to a sensible number depending on the number of locations/customers being planned (i.e. at least 3 digits).
Includes CID	Select this checkbox if you want the CID to be included in the fint. Regardless of whether you select this or not, CIDs are still allocated to Unified CM PBX clusters.
CID Digits	The number of digits to use for the CID. As CIDs are still allocated to Unified CM PBXs even if it's not being used in the fint, this should be set to a sensible number depending on the number of clusters being planned.
Includes Site Code?	Select this checkbox to include the site code in the fint. Regardless of whether you select this or not, Site Codes are still required for locations to be added.
Max. Site Code Digits	This number reflects the maximum number length of the site code.
Site Code Rules	Free text which is displayed next to site codes when they are being added to the system to communicate the rules imposed by the dial plan. This should be useful to the user, for example, <i>Maximum length of 4 digits</i> .

Fields	Description
Variable Length Internal Number?	Select this checkbox if you want the length of the extension portion of the fnt to be configurable. If <i>Variable Length Internal Number</i> is set to <i>Y</i> , the <i>Internal Number Length</i> field must be blank. Enabling this option results in an extension length setting being available during add location. This can be used to define the length of the extension. If this is not selected, the length of the extension is determined by taking the setting below and subtracting any other digits from it (i.e. a location has a site code of 123 (3 digits) and the dial plan calls for no CPID, no RID, and 7 for internal number length. This would result in the extension length being $4 = 7 - 3$.
Internal Number Length	This option enables the user to define the length of the internal number. This is used only if the variable length extension is not enabled. See the entry above to determine the extension length. This is a mandatory field.
Internal Number Display Rules These setting determine how internal numbers are displayed within the application. This drives a value, <i>displayfntnumber</i> , which is used anytime the fnt would be displayed to the user (within the GUI, Self Care, default line text in Unified CM, etc). Note If you change these settings, it does not affect any fnts already in the system. However, it does affect any new fnts added to the system (i.e. locations).	
Includes CPID?	Selecting this checkbox includes the CPID in the number display.
Includes RID?	Selecting this checkbox includes the RID in the number display.
Includes Site Code?	Selecting this checkbox includes the Site Code in the number display.
RID Type Selection	
Routing Identifier (RID)	Use the drop-down list to determine the hierarchy the RID is allocated at. The <i>Location</i> option, is currently the most common choice here.
Dial Prefixes This section covers any dial prefixes that are required for various call types. This allows the requirements to be turned on/off as well as specification of the value.	
Inter-Site Prefix Required?	Select this checkbox if an inter site prefix is required for the dial plan.
Inter-Site Prefix Configurable?	Select this checkbox if the prefix is a configurable value. This is configurable per customer and can be defined for the customer when adding. If not selected then the value used during the Add Customer operation will be hard coded.
PSTN Access Prefix Required?	Select this checkbox if a PSTN breakout code is required.
PSTN Access Prefix Configurable?	Select this checkbox if the prefix is a configurable value. This is configurable per location and can be defined for the location when adding. If not selected then the value used during the Add Location operation is hard coded.

Fields	Description
Call Park Prefix	<p>To distinguish between Call Park numbers internally, the system uses a custom prefix, followed by a number increment, one per call processing server in a Location's Unified CM cluster.</p> <p>The Prefix can be set by the system administrator, either at the System level, where it applies to all Locations (as a default,) or at the individual Location level. It can contain the characters #,* or 0-9, and the existing dial plan should be taken into consideration when assigning it.</p> <p>Because the Prefix is common to all Call Park internal numbers in a Location, the system uses a Sequence Number to ensure that all Call Park numbers are unique in a cluster. Call Park numbers are only created on Unified CM servers marked as Call Processor Engines (CPEs.) For each additional CPE that is targeted during the Call Park create sequence, the Internal Sequence Number portion of the Call Park identifier is incremented by one.</p> <p>Note</p> <p>To manage mega-clusters, which can handle up to 16 subscribers, the sequence number consists of two (2) digits. The sequence numbers range from 01 (for the first server) to 16 for the highest number of servers.</p> <p>For example, if an administrator selects #2 as a Call Park Prefix and creates a 10 number Call Park range, the numbers would be #20100, #20101 etc. on Server A and #20200, #20201 etc. on Server B.</p>
Call Park Location Configurable?	Select this checkbox if the prefix is a configurable value. If selected , the value in the Call Park Prefix field is displayed at a location level in a read-only text field. This is configurable per location and can be defined for the location when adding. If not selected , then the value used during the Add Location operation is hard coded.
Format of External Phone Number Mask on Unified CM <p>This section determines how external (E164/FNN) numbers are displayed in the system. This includes in drop-downs for assigning lines to phones/users and also for configuring the external mask in Unified CM for the lines.</p> <p>Note</p> <p>If you change this setting, it will not affect any FNNs already in the system. The displayed E164 value is determined for the number when it is added to the e164 inventory. It will affect any new FNNs added to the system.</p>	
Show PSTN Dial Prefix	This setting enables the inclusion of the PSTN breakout prefix on the front of the number.
Show Country Code	This setting enables the inclusion of the country code at the beginning of the number (e.g. 44 for the UK).
PSTN Access Prefix Configurable?	Select this checkbox if you would like the PSTN access prefix to be configurable.
Show National Code Prefix	This setting enables the display of the trunk access code on the front of the PSTN number (e.g. 0 for the UK).
Show National Code	This setting enables the display of the area code on the front of the PSTN number.

Fields	Description
Prefix Plus Symbol	This setting enables the inclusion of the international escape character at the beginning of the number.
Format of IPPBX Configured Internal Number This section determines how the FINT numbers are provisioned in the IPPBX system (the DN in Unified CM). This is generally done when you setup a device with an extension number (phones, user extension mobility, CTI, etc). This also affects any features that make use of the FINTs (e.g. Pickup Groups, Hunt Groups, SNR, etc). By default the settings for the <i>Includes SiteCode</i> and <i>Includes Extension</i> checkboxes are selected . Note If you change this setting, it does not affect any FINTs already provisioned in the system. It only affects any new FINTs added to the system. Changes can however be applied to existing locations using the iFint Migrate feature (see the Deployment Guide for more details on this tool). The full list of features that use the iFint logic are: <ul style="list-style-type: none"> • Phone Lines configuration • Extension Mobility Profile (Device Profile) lines • CTI route points - port lines • Analog Port Lines • Pick up Groups - number and members • Number Group (line group in Unified CM) members • Hunt Group Pilot numbers • Location Call Park Numbers • SNR Setup (Remote Destinations, etc) 	
Includes CID	Select this checkbox to include the CID in the external phone number mask.
Includes CPID	Select this checkbox to include the CPID in the external phone number mask.
Includes RID	Select this checkbox to include the RID in the external phone number mask.
Includes SiteCode	Select this checkbox to include the site code in the external phone number mask.
Includes Extension	Select this checkbox to include extensions in the external phone number mask.

Fields	Description
Format of Voicemail Configured Pilot Number This section determines how the Voicemail pilot numbers are provisioned in the IPPBX system (the DN in Unified CMr). The default setting for the <i>Includes Inter-site Prefix</i> checkbox is not selected (OFF) . The default setting for both the <i>Includes SiteCode</i> and the <i>Includes Extension</i> checkboxes is selected (ON) . Note These default settings are critical to ensure backward compatibility when a customer upgrades to a later software version. If you change these default settings, the Voicemail feature for your location will not function. Note Customers that are using only the extension number in their existing system configuration must unselect (switch off) the <i>Includes SiteCode</i> checkbox after performing an upgrade.	
Includes Inter-Site Prefix	Select this checkbox to include the inter-site prefix in the Voicemail pilot number.
Includes SiteCode	Select this checkbox to include the site code in the Voicemail pilot number.
Includes Extension	Select this checkbox to include the extension in the Voicemail pilot number.
Format of Voicemail Configured Mailbox Number This section determines how Voicemail mailbox numbers are provisioned in the IPPBX system (the DN in CallManager). The default setting for both the <i>Includes SiteCode</i> and the <i>Includes Extension</i> checkboxes is selected (ON) . Note These default settings are critical to ensure backward compatibility when a customer upgrades to a later software version. If you change these settings, the Voicemail feature for your location will not function. Note Customers that are using only the extension number in their existing system configuration must unselect (switch off) the <i>Includes SiteCode</i> checkbox after performing an upgrade.	
Includes SiteCode	Select this checkbox to include the site code in the Voicemail mailbox number.
Includes Extension	Select this checkbox to include the extension in the Voicemail mailbox number.

Procedure

Deleting Dial Plans

To delete a Dial Plan:

- Step 1** Browse to *Dial Plan Tools > Number Construction*.
- Step 2** Select the *Name* (active text link) of the Dial plan that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the delete operation, the dial plan is deleted from the system.

Migrate Models

The system's *Migrate Models* functionality enables administrators to initiate the migration of a location(s). Administrators are also able to see the current migration state of locations in the system as well as the migration history for a location. Migration information available for each location includes:

- The version of the system on which the migration was run
- The date and time of the migration
- A user supplied description of the migration

Important: The Migrate Models functionality will migrate all settings and configurations traditionally managed by the system, for 3rd party hardware and software updates, please contact the relevant support person.

Procedure

Accessing the Migrate Models page

To access the *Migrate Models* page:

- Browse to *Dial plan Tools > Migrate Models*.

The *Migrate Models* page lists all relevant location migration information. Administrators are able to search for a location within the list using the system hierarchy and the system's quick search functionality. To filter the list of results, select the required Provider, Reseller, Customer, and Division from the drop-down list along the header of the page. Due to the nature of the system hierarchy, please ensure that you select the drop-down values from left to right.

Information available on this page includes:

Field	Description
<i>Provider Name</i>	Name of the locations Provider
<i>Reseller Name</i>	Name of the locations Reseller
<i>Customer Name</i>	Name of the locations Customer
<i>Division Name</i>	Name of the locations Division
<i>Location Name</i>	Name of the Location
<i>Version</i>	The active system version during the migration
<i>Date</i>	Date and Time that the Location was migrated
<i>Information</i>	Reference provided by user when migrating

Procedure

Migrating a Single Location

To migrate a single location:

- Step 1** Browse to *Dial plan Tools > Migrate Models*.
- Step 2** Using the hierarchy drop-down lists and/or the *Quick Search* functionality to locate the location that you would like to migrate.
- Step 3** Click the **Migrate** button adjacent to the location that you would like to migrate.

Step 4 Enter a comment in the *Description* field.

Note: This is not compulsory but it is recommended that you include a reference here to assist with debugging and the tracking of migrations.

Step 5 Select the required *Migration Features* and *Migration Models* using the supplied checkboxes

Step 6 Click the **Next** button.

Step 7 Review the migration details then click the **Start Migration** button.

The location is migrated. Please ensure to review the transaction status to ensure the migration was successfully.

Procedure

Migrating Multiple Locations

The system enables administrators to select multiple sites and migrate them in a single work flow. For example, all locations in a particular customer can be migrated together.

To migrate multiple locations:

Step 1 Browse to *Dial plan Tools > Migrate Models*.

Step 2 Using the hierarchy drop-down lists and/or the *Quick Search* functionality to locate the locations that you would like to migrate.

Step 3 Select the checkboxes adjacent to the locations that you would like to migrate, then click the **Migrate Selected** button.

Note: To assist with selecting large numbers of locations at once, the system has provided the **Select all** and **Select None** buttons.

Step 4 Enter a default comment in the *Default Description* field. To enter comments for specific locations, locate the location in the list then enter a comment in the description field adjacent to the relevant location.

Note: This is not compulsory but it is recommended that you include a reference here to assist with debugging and the tracking of migrations.

Step 5 Select the required *Migration Features* and *Migration Models* using the supplied checkboxes.

Step 6 Click the **Next** button.

Step 7 Review the migration details then click the **Start Migration** button.

The locations are migrated. Please ensure to review the transaction status to ensure the migration was successful.

Hardware Set Management

Hardware sets are used in conjunction with the hardware groups to determine if alternate configuration needs to be applied to other devices when a device is updated. For these devices, there is a model that is used to define the configuration applied to the other devices in the set. An example would be AddLocation. A location is allocated to an IPPBX and all the configuration is applied there (partitions, CSS, RPs, etc.), however, due to the dial plan design, other PBXs in the system require a site code to be configured on them to point to the correct cluster. This is where the hardware sets can be used to specify that other PBXs that need to be updated as a result of one PBX being updated.

Hardware Sets define the templates for the system to adopt in terms of the types of hardware configurations and they also define the associated dial plans for each hardware set.

There are multiple choices for hardware sets, such as:

- PGW/CCM
- CCM only

In each of the above cases, a different dial plan can be associated, such as:

- Multi-Tenant
- Large Enterprise
- Branch Banking
- Business Park

For example, the Multi-tenant Dial plan must be associated with the PGW/CCM Hardware set, but other variants can have many permutations and combinations.

Procedure

Managing Associated Dial Plans

To manage an associated dial plan:

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Select the **Associated Dial Plan** button adjacent to the Hardware set that you would like to modify.

A list of dial plans is displayed with a short description of each dial plan.

- Step 3** To associate an available dial plan to the active hardware set, click the **Connect** button.

Alternatively,

To disassociate a dial plan from the active hardware set, click the **Disconnect** button.

The dial plans are connected/disconnected from the hardware set.

Add a Hardware Set

Procedure

To add a hardware set:

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields. The following fields are available when adding a hardware set:

Field	Description
Name	The name of the hardware set being added. This is a mandatory field and must be unique in the system.
Description	A short description of the hardware set being added.

Field	Description
Supported Hardware	Select the checkbox adjacent to the name of the hardware device that you would like to include in the hardware set. Multiple hardware devices may be selected at one time.

- Step 4** Click the **Add** button. The hardware set is added to the system and is available in all relevant menus.

Viewing and Modifying a Hardware Set

Procedure

To view and modify a Hardware Set:

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Select the *Hardware Set* (active text link) that you would like to modify.
- Step 3** Complete the required fields and click the **Modify** button.

The fields that are available when modifying a Hardware Set are as in [Add a Hardware Set on page 70](#).

The Hardware Set is modified within the system.

Procedure

Deleting a Hardware Set

To delete a Hardware Set:

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Select the *Hardware Set* (active text link) that you would like to delete.
- Step 3** Click the **Delete** button.

After confirmation, the Hardware Set is deleted from the system.

Connect (Associate)/Disconnect (Disassociate) a Dial Plan to the Hardware Set

Procedure

To associate a dial plan to a hardware set:

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Click the **Associated Dial Plan** button adjacent to the hardware set that you would like to modify. A list of dial plans is displayed with a short description of each dial plan.
- Step 3** Click the **Connect** button to associate an available dial plan to the active hardware set, OR click the **Disconnect** button to disassociate a dial plan from the active hardware set. The dial plans are connected/disconnected to/from the hardware set.

Loading the Dial Plan Models

Procedure

The next step is to load the required models, for example, the Unified CM model. To upload models to the system:

Step 1 Browse to *Dial Plan Tools > Configuration Models > Model Loader*.

Step 2 Click the **Schedule new job** button.

Step 3 Click the **Browse** button and select the Spreadsheet (model) that you would like to upload.

Note

- The system currently supports the uploading of Microsoft™ Excel © *.xml spreadsheets.
- Sample Models can be downloaded by browsing to Dial Plan Tools > Configuration Models > <Select required subset>.

Step 4 Specify the specific date and time when you would like to execute the model loader task. This is specified as yyyy-mm-dd and hh:mm:ss, or select the *Execute as soon as possible* checkbox if you would like the model loader task to run as soon as possible. In these instances, the model load task/s is scheduled to run in the order in which they were submitted.

Note

If you want the selected model load task to run immediately, regardless of those already running, and with no consideration for dependencies, select the *Execute immediately* checkbox.

Step 5 Select the relevant file encoding type from the drop-down list, and then click the **Submit** button to schedule the upload. We recommend that you always review any errors or warnings received at the completion of loading.

Viewing Pending Config Model Upload Jobs

To view pending, running, and completed config upload jobs, browse to the *Configuration Models* page under the *Dial Plan Tools* menu. The page lists all config model upload jobs that are scheduled, running and have completed. Jobs can have one of five states:

- **Scheduled:**

This status indicates the scheduled time of the load has not occurred yet. The load starts at the time scheduled.

- **Validating:**

The load process is validating the data in the workbook. This occurs before any loading occurs. The current sheet being validated can be seen on the details page for that load. The whole workbook is validated and if there are any errors the load does not progress to the next phase. The details of the validation failures can be seen in the log.

- **Loading:**

This status indicates the process has passed validation and is starting transactions. The current sheet and row being worked on can be seen on the details page for the load. The transactions being started can be seen via the **Show Transactions** button.

- **Completed:**

This status means the load process has completed processing the data in the sheets. The errors count indicates how many of the transactions the loader initiated did not complete successfully. The details of the transactions can be seen in the transaction log or the **Show Transactions** button.

- **Failed:**

Generally means the load process hit some internal issue in the load process. The log file for the load can be seen for more details.

To view further information about config upload jobs, select either the Job number or the name of the spreadsheet uploaded. From the *Config Model Details* page you are able to view details of the upload job. To view details of the individual transactions related to the upload job, click the **Transactions** button.

For further details on what information was uploaded and if any errors were reported during the upload process, click the **Show Details** button. To view the log relating to the upload job, select the *Log* active text link.

Adding a Provider(s)

The system enables multiple service providers to be added to the same platform. The provider management section enables the creating, modification and deleting of the each of the service providers.

Procedure

Follow these steps to add a new provider in the system:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Click the **Add** button on the *Provider Management* screen.
- Step 3** Complete all of the required details. The available fields include:

Name	The name of the Service Provider.	This must be alpha numeric and is a mandatory field.
Description	A description of the Service Provider	-
Address1	Address of the Service Provider.	This is a mandatory field.
Address2	Address of the Service Provider.	This is a mandatory field.
Address3	Address of the Service Provider.	This is a mandatory field.
City	City where the Service Provider is situated.	This is a mandatory field.
State	State where the Service Provider is situated.	-
Country	Country where the Service Provider is situated.	This is a mandatory field. Select the country from the drop-down list.
Post/ZIP Code	Post (Zip) code where the Service Provider is situated.	This is a mandatory field.
Contact Name	Contact Name for the person responsible for the provider.	This is a mandatory field.
Contact Telephone Number	Contact telephone number for the person responsible for the provider.	This is a mandatory field.
Contact Email	Contact email address for the person responsible for the provider.	-
Account number to use in external accounting system	The account number to be used for an external accounting system.	This is an optional field. Specify as required.

Name	The name of the Service Provider.	This must be alpha numeric and is a mandatory field.
Security Profile	The selected security profile.	Select from the drop-down list.
Type of Hardware Deployed	Defines the major components used by this Service Provider and the associated Dial Plan.	This is a mandatory field. Select the required hardware set from the drop-down list.
Default Branding of User Interface	Defines the default branding to be used with this Service Provider.	This is a mandatory field.
Select required Branding:	The branding that are going to be available to the Service Provider.	Select the checkboxes adjacent to the branding that are going to be available to the Service Provider.

Step 4 Click the **Add** button. The new provider is created within the system.

Managing Provider Preferences

Procedure

To modify provider preferences in the system:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the *Provider* (active text link) that you would like to modify.
- Step 3** Click the **Preferences** button.
- Step 4** Select the relevant preference (active text link).
- Step 5** Select the checkbox then click the **Modify** button. The system is updated.

International Gateway Usage

Procedure

Follow these steps to add a country to an international gateway in the system:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the *Provider* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **International Gateway Usage** button.
- Step 5** Select the relevant *Transit Switch* (active text link).
- Step 6** Click the **Add** button adjacent to the country that you would like to add.
- Step 7** Provide all of the required fields. Available fields include:

Field	Description
Country	Select the country you would like to add from the drop-down list. This is a mandatory field.
National Code	Supply the national code for the country being added. Please ensure that the correct, and entire, code is supplied.

Field	Description
Gateway Usage	Select the relevant radio checkbox, only one option may be selected. Options include Force Central and Allow Local. This is a mandatory field.

Note

The transaction adds the country to the system database as well as add settings to the PGW. The PGW settings are model driven:

- Adding a country with the *Force Central* setting selected provisions the PGW driver via the *AddTransitForceCentral* PGW model.
- Adding a country with the *Allow Local* setting selected provisions the PGW driver via the *AddTransitAllowLGW* PGW model.

Step 8 Click the **Add** button. The country is added to the Gateway.

Gatekeeper Management

A Gatekeeper is a device used to manage the bandwidth requirements between Call Managers and the Transit Switch. There must be a Gatekeeper for each Call Manager Cluster.

Note

You must be at the Service Provider Administrator security level, or higher, to add, delete or modify a Gatekeeper.

Procedure***Adding a Gatekeeper***

To add a Gatekeeper:

- Step 1** Browse to *Network > Gatekeepers*.
- Step 2** Click the **Add** button.
- Step 3** Select the required Gatekeeper type.
- Step 4** Complete the required fields and click the **Add** button.

The Gatekeeper is added to the system.

Procedure***Modifying a Gatekeeper***

To modify a Gatekeeper:

- Step 1** Browse to *Network > Gatekeepers*.
- Step 2** Select the *Name* (active text link) of the Gatekeeper that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button. The Gatekeeper is updated with the changes.

Deleting a Gatekeeper

To delete a Gatekeeper:

- Step 4** Browse to *Network > Gatekeeper*.
- Step 5** Select the *Name* (active text link) of the Gatekeeper that you would like to delete.
- Step 6** Click the **Delete** button.

After confirming the deletion, the Gatekeeper is removed from the system.

Procedure

Testing the Gatekeeper

To test a Gatekeeper:

- Step 1** Browse to *Network > Gatekeepers*.
- Step 2** Select the *Name* (active text link) of the Gatekeeper that you would like to test.
- Step 3** Click the **Test** button.

The Gatekeeper is tested and the results displayed on screen.

Procedure

Adding a Gatekeeper(s)

To add a Gatekeeper in the system:

- Step 1** Browse to *Network > Gatekeepers*.
- Step 2** Click the **Add** button.
- Step 3** Select the required Gatekeeper type.
- Step 4** Complete the required fields. For information on available fields, see the table under [Available Server Fields on page 919](#) if required.
- Step 5** Click the **Add** button. The gatekeeper is added to the system.

Add a Cisco 36xx Gatekeeper

Procedure

To add a Cisco 36xx Gatekeeper:

- Step 1** Browse to the relevant sub-menu under the *Network* menu.
- Step 2** Click the **Add** button.
- Step 3** If asked to specify what type of Server you would like to add, click the **Add** button adjacent to the Server type that you would like to add. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and click the **Add** button.

The Cisco 36xx Gatekeeper is added to the system.

The following fields are available when adding a Cisco 36xx Gatekeeper:

Note: Depending on the configuration of your system, some of these fields may not be available

Field	Description
<i>Host Name</i>	Must be unique in the system. This is a mandatory field.
<i>IP Address</i>	The IP address of the server being added. The IP address must be unique within the system. This is a mandatory field.
<i>Description</i>	A short description of the server.
<i>Cisco User Id Required?</i>	Select this checkbox if you would like to force users to use a Cisco User ID to access the server.
<i>Config User name</i>	The user name for configuring the server. This is a mandatory field.
<i>Config Password</i>	The password to be used when configuring the server. This is a mandatory field.
<i>Enable Password</i>	Select this checkbox to force the use of the password.
<i>Version</i>	Select the version of server from the drop-down list.
<i>Manual Configuration Mode?</i>	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
<i>Email address for Manual activation</i>	The email address that will be used for manual activation of the CCM Server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
<i>Network Monitoring active?</i>	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
<i>Detailed trace file of configuration sessions?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Encrypt configuration sessions?</i>	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.

Cisco 36xx Server Tools

Server Tools enable administrators to perform advanced operations on Cisco 36xx Servers. For more information on the available tools, please consult the relevant Feature Guide.

View and Modify a Cisco 36xx Gatekeeper

From the *View and Modify a Cisco 36xx Gatekeeper* screen, the following tools are accessible:

Tool/Task	Accessed Via	Description
<i>Test</i>	Click the Test button.	A test of the server occurs immediately and the results of the test are displayed.
<i>Load</i>	Click the Load button.	The server is loaded immediately using the specified IOS scripts. Important: No confirmation is requested during this operation.
<i>Server Modification</i>	Make the required changes and click the Modify button.	For more information, see the Modify section below.
<i>Delete</i>	Click the Delete button.	This deletes the server from your system. Important: Depending on the configuration of your system, confirmation may be requested prior to deleting a server.

Procedure

To modify a Cisco 36xx Gatekeeper:

- Step 1** Browse to the relevant sub-menu under the *Network* menu.
- Step 2** Select the *Name* (active text Link) of the server that you would like to modify.
- Step 3** Modify the required fields then click the **Modify** button.

The Cisco 36xx Gatekeeper is modified in the system.

The following fields are available when modifying a Cisco 36xx Gatekeeper:

Note

Depending on the configuration of your system, some of these fields may not be available.

Field	Description
<i>Host Name</i>	Must be unique in the system. This is a mandatory field.
<i>IP Address</i>	The IP address of the server being added. The IP address must be unique within the system. This is a mandatory field.
<i>Description</i>	A short description of the server.
<i>Cisco User Id Required?</i>	Select this checkbox if you would like to force users to use a Cisco User ID to access the server.
<i>Config User name</i>	The user name for configuring the server. This is a mandatory field.
<i>Config Password</i>	The password to be used when configuring the server. This is a mandatory field.
<i>Enable Password</i>	Select this checkbox to force the use of the password.
<i>Version</i>	Select the version of server from the drop-down list.
<i>Manual Configuration Mode?</i>	Select this checkbox if you would like the server to operate in manual configuration mode. This option should be selected for un-managed clusters. It is mandatory to supply an email address if this option is selected.
<i>Email address for Manual activation</i>	The email address that will be used for manual activation of the CCM Server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
<i>Network Monitoring active?</i>	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
<i>Detailed trace file of configuration sessions?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Encrypt configuration sessions?</i>	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.

H323 Links

Note

This section only applies if multiple gatekeepers are being used.

A Gatekeeper can be associated with a Gatekeeper(s).

Procedure

Viewing associated Gatekeepers

To view Gatekeepers currently associated to the selected Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu
 - Step 2** Select the **H323==>H323 Links** button adjacent to the Gatekeeper that you would like to view
- A screen will be displayed, with two columns, one listing the registered (and available) Gatekeepers, and the other column will display the Gatekeepers current connection status. If the button adjacent to the Gatekeeper says **Connect**, the Gatekeeper is available for connection. If the button says **Disconnect**, the Gatekeeper is already connected.

Procedure

Associating (connecting) a Gatekeeper to a Gatekeeper

To associate a Gatekeeper to a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **H323==>H323 Links** button adjacent to the Gatekeeper that you would like to associate.
- Step 3** Select the **Connect** button Adjacent to the Gatekeeper that you would like to associate with the Gatekeeper.

The Gatekeeper will now be associated with the selected Gatekeeper.

Procedure

Disassociating (disconnecting) a Gatekeeper from a Gatekeeper

To disassociate a Gatekeeper from a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **H323==>H323 Links** button adjacent to the Gatekeeper that you would like to disassociate from a Gatekeeper(s).
- Step 3** Select the **Disconnect** button Adjacent to the Gatekeeper that you would like to disassociate from the Gatekeeper.

The Gatekeeper will now be disassociated from the selected Gatekeeper.

Add a PGW (Transit Switch)

Procedure

To add a PGW server:

- Step 1** Browse to *Network > Transit Switches*.

- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the PGW server if you are asked to specify what type of server you would like to add.
- Step 4** Complete all of the required fields. For information on available fields, see the table under [Available Server Fields on page 919](#) if required.
- Step 5** Click the **Add** button. The PGW server is added to the system.
-

Associating a PGW to a Gatekeeper

Procedure

To associate a Transit Server to a Gatekeeper:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit**⇒**Gatekeeper** button adjacent to the PGW that you would like to associate.
- Step 3** Click the **Connect** button adjacent to the gatekeeper that you would like to associate with the transit server. The transit server is associated with the selected gatekeeper.
-

Adding Cisco Unified CM Clusters

Adding a CCM

Note

In the case of LDAP integrated environments, please refer to the *LDAP Integration Guide* for details on key configuration steps on Unified CM.

Procedure

To add a CCM server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to CCM Server.
- Step 4** Complete all of the required fields. For information on available fields, see the table under [Available Server Fields on page 919](#) if required.
- Step 5** Click the **Add** button. The CCM server is added to the system.
-

Note

When configuring CCM server details in the system, it is critical to ensure that the fields are completed correctly. Two of the most important fields include the *Hostname* and *CCM Name* fields:

- **Hostname:**

This must be the actual hostname of the server (if Cisco Unified Communications Manager (Unified CM) 5.X or later, it must not be an IP Address). If you have any doubt, the hostname of the server in 5.x onwards

can be determined with the Unified CM CLI command `show network cluster`, it is the value in the 2nd column.

- **CCM Name:**

This must be the name of the server as shown in Unified CM (typically the IP Address of the server). This value is found by browsing to System -> Cisco Unified CM. The CCM Name field is also referred to as the Publisher CCM Name field on the AddCluster screen and in the loaders.

CCM Server Management

Adding a Server to a Cluster

Procedure

Adding a Server to a Cluster

To add a Server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *PBX Server Name* (active text link) of the CCM cluster to which you would like to add a server.
- Step 3** Click the **Servers** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required fields. The following fields are available when adding a Server to a CCM cluster:

Note: Depending on the configuration of your system, available fields may vary.

Field	Description
<i>Host Name</i>	Hostname for the server where the Unified CM is installed. This is a mandatory field. To maintain parity with the Unified CM, the host name in CUCDM must contain only letters, numbers and dashes, and must end with either a letter or a number.
<i>CCM Name</i>	CCM name for the server where the Unified Communications Manager is installed. This is a mandatory field.
<i>Description</i>	A short description of the server.
<i>IP Address *</i>	This is the IP address used by CUCDM when communicating with the Unified CM server. This is only true for the publisher. This is also the address that is used to create trunks (publisher and subscribers) between PBXs.
<i>IP Address B</i>	This IP address is available for use by Gateways when communicating with the Unified CM server. A Gateway option allows the user to specify whether the normal IP Address or this address is used. This allows support for various NAT configurations. See the IOS Gateways Guide for details on how to use these settings/options.
<i>EMCC Server</i>	Select this checkbox if this server is going to be used as a EMCC. If this option is selected, please provide the order for the server (see adjacent drop-down list).
<i>TFTP Server</i>	Select this checkbox if this server is going to be used as a TFTP. If this option is selected, please provide the order for the server (see adjacent drop-down list).

Field	Description
<i>Music Server</i>	Select this checkbox if this server is going to be used as a Music server. If this option is selected, please provide the order for the server (see adjacent drop-down list).
<i>Conference Server</i>	Select this checkbox if this server is going to be used as a Conference Server.
<i>Annunciator Server</i>	Select this checkbox if this server is going to be used as a Annunciator Server.
<i>Media Termination Point Server</i>	Select this checkbox if this server is going to be used as a Media Termination Point Server.
<i>Attendant Console Server</i>	Select this checkbox if this server is going to be used as a Attendant console Server.
<i>CTI Manager Server</i>	Select this checkbox if this server is going to be used as a CTI Manager Server.
<i>MGCP Configured</i>	Select this checkbox if MGCP has been configured.
<i>H323 Configured</i>	Select this checkbox if H323 has been configured.
<i>SCCP Configured</i>	Select this checkbox if SCCP has been configured.
<i>SIP Configured</i>	Select this checkbox if SIP has been configured.
<i>Call Processor Engine</i>	Select this checkbox if the call processor engine has been configured.
<i>Network Monitoring active?</i>	Select this checkbox if you would like the server to activate Network Monitoring. Note Depending on network loads, selecting this option may impact on the performance of the server.

Step 6 Click the **Submit** button when complete. The server is added to the CCM cluster.

Note

The identical host name in CUCDM (see *Host Name* field above) must exist in Unified CM. If it does not already exist, it must be manually created in Unified CM (see under *System > Server* in the Unified CM).

Unified CM Group Management

Adding a Group

Procedure

To create a new group within a cluster:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Select the *Name* (active text link) of the Unified CM cluster to which you would like to add a group.
- Step 3** Click the **Groups** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields and click the **Submit** button.

The group is added to the system.

The following fields are available when adding a group:

Field	Description
Group Name	The name of the group being added. This is a mandatory field.
Description	A short description of the group
Maximum Streams supported	Specify the maximum number of streams supported by the group. This is a mandatory field.
Use for Phones	Select this checkbox if this group is going to be used for phones.
Use For Trunks	Select this checkbox if this group is going to be used for Trunks.
Use For Voicemail	Select this checkbox if this group is going to be used for voicemail.
Select Servers	Select the checkbox(s) adjacent to the servers that you would like to appear in this group.
Server Order	Use the drop-down list to specify the hierarchy of the servers, for example, if you would like <i>Server 1</i> to be before <i>Server 2</i> , you would select <i>1</i> from the drop-down list adjacent to <i>Server 1</i> and you would select <i>2</i> from the drop-down list adjacent to <i>Server 2</i> . Important: The server orders must be unique within the group. For example, two or more servers cannot be on order 0. All servers must have a unique order number assigned to them.

Cluster Management - Attribute Management

This screen lists all of the attributes and associated attribute values related to the cluster. To modify multiple attributes and values, make the required changes on the required attributes, and then click the **Modify All** button.

Note

The *Query* transaction retrieves the existing attribute values from Unified CM.

To query multiple attributes values, click the **Query All** button.

The following columns are available:

Column	Description
Name	The name of the attribute.
Current Setting	The current status/value of the attribute. Note that the available options for this setting are not presented in drop-down lists as these cannot be retrieved from Unified CM. They may also differ between different versions of Unified CM.
Type of Service	The type of service.

Procedure

Modifying an Attribute

To modify an attribute:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the group that you want to modify.
- Step 3** Click the **Attributes** button.
- Step 4** Locate the attribute *Name* that you want to modify.
- Step 5** Modify the required attribute values, that is the *Current Setting* status checkbox (selected - enabled or not selected - disabled), or the current attribute text field (as appropriate).
- Step 6** Click the **Modify** button adjacent when complete. The attribute is modified.

Note

Alternatively, select the required attribute *Name* (active text link), modify the value (as described in step 5 above) on the specific attribute screen and then click the **Modify** button.

Procedure

Querying an Attribute

To query (retrieve value from Unified CM) an attribute:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the group that you would like to query.
- Step 3** Click the **Attributes** button.
- Step 4** Click the **Query** button adjacent to the attribute that you would like to query. The results of the query are displayed.

Bandwidth Groups

Bandwidths can be configured directly on the location instead of on an IP edge device linked via a subnet.

Bandwidth Groups can be created to allow locations to share bandwidth pools. This replaces the previous mechanism which was via IP edge devices common to locations.

The user can create and manage bandwidth groups, which are then used to configure bandwidths at locations. Bandwidth groups are configured at a PBX device. Locations that have the same bandwidth group share the same bandwidth pool.

From the *Bandwidth Groups* screen, you can add (new), as well as view, modify and/or delete (existing) bandwidth groups.

Existing Bandwidth Groups are listed on the *Bandwidth Groups* screen under the following headings:

Field	Description
Name	The name of the bandwidth group.

Field	Description
Description	A brief description of the bandwidth group.
Voice Bandwidth (kbps)	The allowed voice bandwidth group in kbps for the Location, for example 512 or 1024. Note that <i>Unlimited</i> indicates an unlimited voice bandwidth.
Video Bandwidth (kbps)	The allowed video bandwidth group in kbps for the Location, for example 512 or 1024. Note that <i>None</i> indicates that there is no video bandwidth allocated at the Location, and <i>Unlimited</i> indicates an unlimited video bandwidth.

- To add a new bandwidth group, click the **Add** button.
- To modify an existing bandwidth group, click the required bandwidth group *Name* (active text link).
- To delete an existing bandwidth group (if not being used by a Location), click the **Delete** button adjacent to the required bandwidth group.

Adding a Bandwidth Group

Bandwidth Groups can be created to allow locations to share bandwidth pools. This replaces the previous mechanism which was via IP edge devices common to locations.

The user can create and manage bandwidth groups, which are then used to configure bandwidths at locations. Bandwidth groups are configured at a PBX device. Locations that have the same bandwidth group share the same bandwidth pool.

Procedure

To add bandwidth group to a cluster:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster to which you would like to add a bandwidth group.
- Step 3** Click the **Bandwidth Groups** button. The *Bandwidth Groups* screen is displayed.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields. The following fields are available when adding a bandwidth group:

Field	Description	Remarks
Name	The name of the bandwidth group being added.	This is a mandatory field.
Description	A short description of the bandwidth group.	-
Voice Bandwidth (kbps)	The allowed voice bandwidth group in kbps for the Location.	Enter the required voice bandwidth for the location. Select the <i>Unlimited</i> radio button for an unlimited voice bandwidth, or enter a specific voice bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field). This is a mandatory field.

Field	Description	Remarks
Video Bandwidth (kbps)	The allowed video bandwidth group in kbps for the Location.	Enter the required video bandwidth for the location. Select the <i>None</i> radio button for no video bandwidth, select the <i>Unlimited</i> radio button for an unlimited video bandwidth or enter a specific video bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field). This is a mandatory field.

Step 6 Click the **Submit** button. The bandwidth group is added to the system.

Bandwidth Group Management

Procedure

To modify a bandwidth group:

- Step 1** Browse to *Network > PBX Devices*. The *Manage PBX Server* screen is displayed.
- Step 2** Select the required PBX Server *Name* (active text link) to which you want to add bandwidth group/s. The *CCM Cluster Management* screen is displayed.
- Step 3** Click the **Bandwidth Groups** button. The *Bandwidth Groups* screen is displayed.
- Step 4** Select the required Bandwidth Group *Name* (active text link) that you want to modify. The *Bandwidth Group Management* screen is displayed.
- Step 5** Modify the required fields. The following table lists and describes the fields available on the *Bandwidth Group Management* screen.

Field	Description
Name	The name of the bandwidth group. This is a mandatory field.
Description	A brief description of the bandwidth group.
Voice Bandwidth (kbps)	The required voice bandwidth for the location. Select the <i>Unlimited</i> radio button for an unlimited voice bandwidth, or enter a specific voice bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field). This is a mandatory field.
Video Bandwidth (kbps)	The required video bandwidth for the location. Select the <i>None</i> radio button for no video bandwidth at the location, or select the <i>Unlimited</i> radio button for an unlimited video bandwidth, or enter a specific video bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field). This is a mandatory field.

Step 6 Click the **Modify** button when complete. The bandwidth group is updated within the system.

Note

If you want to delete the selected Bandwidth Group, click the **Delete** button at the bottom-right of the screen. You can only delete bandwidth groups that are **not** used by a location.

Importing/Refreshing CCM Items

Various CCM items can be imported/refreshed in the system from Cisco Unified Communications Manager (Unified CM), these include:

Note

- Attributes
- Date/Time Groups. **Note:** Date/Time groups must be imported from Unified CM before a device pool template, device pool or a location can be added. Device pools that were migrated because they existed before the introduction of this feature are operational and behave as before, but modifying these device pools is not possible until Date/Time groups are imported.
- Discard Digits
- Feature Control Policies
- Phone Button Templates
- Phone Features
- Phone Security Profiles. **Note:** Phone security profiles must be imported from Unified CM before registering or modifying a phone to ensure that the latest available phone security profile options are displayed in the *Phone Security Profile* drop-down list on the *Phone Registration* and *Phone Management* screen.
- Recording Profiles
- Service Parameters
- SIP Normalization Scripts
- SIP Profiles
- Softkey Templates
- User Locales

Procedure

To import/refresh CCM items:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Select the *Name* (active text link) of the CCM cluster that you would like to modify.
 - Step 3** Click the **Import/Refresh Items** button.
 - Step 4** Select the checkbox adjacent to the item(s) that you would like to import/refresh and click the **Import/Refresh Items** button. The selected items are imported into, or refreshed in the cluster.
-

See also: [Viewing CCM Items on page 88](#)

Media Services Management

Media resources include media resource groups and media resource group lists. Media resource management enables all CCMs in a cluster to share media resources including conferencing, transcoding, media termination, annunciator, and MOH services. Media resource groups and media resource group lists are added per CCM cluster.

When managing the configuration of Call Manager and Media Services, you are required to specify what aspect of media you would like to add, modify or delete.

Follow the step that is most appropriate to you below:

- To configure customers, select the **Customer Config.** button
- To configure media resource groups, select the **Media Resource Groups** button
- To configure Media Resource Group Lists, select the **Media Resource Group Lists** button

Note: Depending on the configuration of your system, you may be presented with alternate options.

Trunk Management

This setting does not apply to Cisco HCS.

Viewing CCM Items

Procedure

To view CCM items:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *Name* (active text link) of the CCM cluster.
- Step 3** Click the **Import/Refresh Items** button. A list of CCM items is displayed.
- Step 4** Select the *Name* (active text link) of the the CCM item that you wish to view. The resultant page enables administrators to gain an overview of a CCM item prior to the item being imported into the cluster.

Each page specifies the Call Manager Cluster name and the name of the CCM Item being viewed. Beneath the CCM item information is a details section that lists the details of the CCM item. The following fields are available when viewing a CCM item:

Note

Depending on the type of item being displayed, the available fields may vary.

Field	Description
S. No	The S.No of the CCM item.
Attribute Name	The name of the CCM item.
Date Type	The type of data related to the CCM item.
Type of Service	The type of service provided by the CCM item.
External ID	The external ID of the CCM item.

Associate an IPPBX to a Gatekeeper

Procedure

To associate an IPPBX to a gatekeeper:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==>Gatekeeper** button.
- Step 4** Click the **Connect** button adjacent to the Gatekeeper that you would like to associate with the IPPBX. The IPPBX is associated with the selected gatekeeper.

Adding a CTI Manager Group

Procedure

To add a CTI Manager Group:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **CTI Manager Group** button adjacent to the IPPBX that you would like to add the CTI Manager Group to.
- Step 3** Click the **Add** button.
- Step 4** Complete all of the required fields. The following fields are available when adding a new CTI Manager Group:

Field	Notes	Remarks
CTI Manager Group Name	The name of the CTI Manager Group Name.	This is a mandatory field.
Primary Subscriber	The Primary Subscriber (CCM server) associated with this CTI Manager Group.	This is a mandatory field. Note To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.
Secondary Subscriber	The Secondary Subscriber (CCM server) associated with this CTI Manager Group.	The Secondary Subscriber is used if the Primary Subscriber is offline. Note To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.
Maximum Connection Capacity	The maximum number of devices that can be associated with this CTI Manager Group.	This is a mandatory field.

- Step 5** Click the **Add** button. On clicking the **Add** button, the following back-end transaction is triggered:
 - AddCTIManagerGroup (for more information see the UC Central Provisioning Guide).

Adding a CTI Manager Group

Procedure

To add a CTI Manager Group:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **CTI Manager Group** button adjacent to the IPPBX that you would like to add the CTI Manager Group to.
- Step 3** Click the **Add** button.

- Step 4** Complete all of the required fields. The following fields are available when adding a new CTI Manager Group:

Field	Notes	Remarks
CTI Manager Group Name	The name of the CTI Manager Group Name.	This is a mandatory field.
Primary Subscriber	The Primary Subscriber (CCM server) associated with this CTI Manager Group.	This is a mandatory field. Note To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.
Secondary Subscriber	The Secondary Subscriber (CCM server) associated with this CTI Manager Group.	The Secondary Subscriber is used if the Primary Subscriber is offline. Note To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.
Maximum Connection Capacity	The maximum number of devices that can be associated with this CTI Manager Group.	This is a mandatory field.

- Step 5** Click the **Add** button. On clicking the **Add** button, the following back-end transaction is triggered:

- AddCTIManagerGroup (for more information see the UC Central Provisioning Guide).

Modifying a CTI Manager Group

Procedure

To modify a CTI Manager Group:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **CTI Manager Group** button adjacent to the IPPBX that you would like to modify.
- Step 3** Select the *Name* (active text link) of the CTI Manager Group that you would like to modify.
- Step 4** Modify the required fields. The following fields are available when modifying a CTI Manager Group:

Field	Notes	Remarks
CTI Manager Group Name	The name of the CTI Manager Group Name.	This is a mandatory field.
Primary Subscriber	The Primary Subscriber (CCM server) associated with this CTI Manager Group.	This is a mandatory field. Note To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.

Field	Notes	Remarks
Secondary Subscriber	The Secondary Subscriber (CCM server) associated with this CTI Manager Group.	<p>The Secondary Subscriber is used if the Primary Subscriber is offline.</p> <p>Note</p> <p>To be available here as a Subscriber, a server in the CCM cluster must be enabled as a CTI Manager Server.</p>
Application User	The name of the Application User associated with this CTI Manager.	-
Application User Type	The associated Application User's type, e.g. UC Central.	-
Maximum Connection Capacity	The maximum number of devices that can be associated with this CTI Manager Group.	<p>This is a mandatory field.</p> <p>Note</p> <p>Adjacent to Maximum Connection Capacity is an indication of Used Capacity, which indicates how many devices have already been connected to the CTI Manager Group.</p>

Step 5 Click the **Modify** button. On clicking the **Modify** button, the following back-end transaction is triggered:

- ModCTIManagerGroup (for more information see the UC Central Provisioning Guide).

Deleting a CTI Manager Group:

Procedure

To delete a CTI Manager Group:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **CTI Manager Group** button adjacent to the IPPBX that you would like to modify.
- Step 3** Select the *Name* of the CTI Manager Group that you would like to delete.
- Step 4** Click the **Delete** button. On clicking the **Delete** button, the following back-end transaction is triggered:
 - DelCTIManagerGroup (for more information see the UC Central Provisioning Guide).

Application User Management

Procedure

Adding an Application User

To add an application user:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to add the application user to.
- Step 3** Click the **Add** button.
- Step 4** Complete all of the required fields. The following fields are available when adding a new application user:

Field	Description	Remarks
Username	The name of the user being added.	This is a mandatory field. Note The system automatically converts Usernames to lower-case and ignores trailing spaces.
Description	An optional description of the user.	-
Enter Password	The password for the application user.	This is a mandatory field.
Confirm Password	The password for the application user re-entered.	This is a mandatory field.
Digest Credentials	Enter a string of alphanumeric characters.	Unified CM uses the digest credentials specified here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you associate the phone to the end user.
Confirm Digest Credentials	Re-enter the above credentials to confirm that you entered the digest credentials correctly.	This is a mandatory field.
Application User Type	Select the required application user type from the drop-down list.	This is a mandatory field.

- Step 5** Click the **Add** button. The application user is added to the system.

Procedure

Modifying an Application User

To modify an application user:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
- Step 3** Select the *Username* of the user that you would like to modify.
- Step 4** Modify the required fields' then click the **Modify** button. The application user is modified within the system.

Procedure

Deleting an Application User

To delete an application user:

- Step 1** Browse to the *Network > PBX Devices*.
 - Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Select the *Name* of the user that you would like to delete.
 - Step 4** Click the **Delete** button. The application user is deleted from the system.
-

Procedure

Modifying an Application User's Digest Credentials

To modify an application user's digest credentials:

- Step 1** Browse to the *Network > PBX Devices*.
 - Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Select the *Name* of the user that you would like to modify.
 - Step 4** Click the **Change Digest Credentials** button.
 - Step 5** Specify the new password, after re-entering it, click the **Submit** button. The application user's digest credentials are updated.
-

Procedure

Modifying an Application User's Password

To modify an application user's password:

- Step 1** Browse to the *Network > PBX Devices*.
 - Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Select the *Name* of the user that you would like to modify.
 - Step 4** Click the **Change Password** button.
 - Step 5** Specify the new password, after re-entering it, click the **Submit** button. The application user's password is updated.
-

Procedure

Associating Devices to an Application User

To modify an application user's associated devices:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
- Step 3** Select the *Name* of the user that you would like to modify.

- Step 4** Click the **Associate Devices** button.
- Step 5** Select the checkboxes adjacent to the devices that you would like to associate then click the **Submit** button. The application user's associated devices are updated.

Note

To assist with managing large numbers of devices, use the **Select All** and **Deselect All** buttons to select or deselect all of the devices on the page.

Procedure

Disassociating Devices from an Application User

To modify an application user's associated devices:

- Step 1** Browse to the *Network > PBX Devices*.
- Step 2** Click the **Application Users** button adjacent to the IPPBX that you would like to modify.
- Step 3** Select the *Name* of the user that you would like to modify.
- Step 4** Click the **Disassociate Devices** button.
- Step 5** Select the checkboxes adjacent to the devices that you would like to disassociate, and then click the **Submit** button. The application user's associated devices are updated.

Note

To assist with managing large numbers of devices, use the **Select All** and **Deselect All** buttons to select or deselect all of the devices on the page.

CCM Server Configuration

This page lists all configured locations and their relevant customers, providers, resellers, customers and divisions.

The information provided on this page includes:

Column	Description
<i>Location Name</i>	The name of the location
<i>Provider Name</i>	The name of the provider responsible for the location
<i>Reseller Name</i>	The name of the reseller responsible for the location
<i>Customer Name</i>	The name of a customer at the location. A single location may have multiple customers.
<i>Division Name</i>	The name of a division within the location.
<i>Address</i>	The address of the Division within the location.

To view further information on a specific location, select the **Location Name** (active text link) of the location.

Selecting the Server Type to Add

Depending on the function of the server being added, you may be asked to specify the type of server that you would like to add.

To select the relevant server type, click the **Add** button adjacent to the server type that you would like to add.

The *Add Server* dialogue appropriate to the server type that you selected is displayed.

Note

Depending on how your system has been configured, and the primary role of the server being added, the list of available servers may differ.

The following server types are available:

Server Type	Description
CCM	The Cisco Call Manager, one of Cisco's foundation Unified communication offerings.
SME	A Cisco Unified Session Manager Edition (Cisco SME) is a transit switch used to aggregate multiple unified communications systems, referred to as leaf systems.
Cisco36xx	A Cisco 36xx Series Router.
CiscoEmergencyResponder	Cisco Emergency Responder ensures that the Cisco Unified Communications Manager (Unified CM) sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.
CiscoSRST	Cisco Secure Survivable Remote Site Telephony. A disaster mitigation technology.
Cisco Unity Connection	Cisco Unity Connection provides integrated messaging to assist users manage communications using their phone, PC or both.
IPUnity	IP Unity is a leader in carrier-grade media servers, application servers and real-time multimedia applications for IP and TDM networks.
WebEx	WebEx conference servers from Cisco are hosted servers to which end users can connect via the system's user interface.
ISC	The Cisco IP Solution Center (ISC). A security management solution from Cisco.
Netwise	A Netwise CMG Telephony Server.
PGW Cisco Transit switch	The Cisco PGW (Protocol Gateway) is a multi-protocol, carrier-grade soft-switch designed to support media gateway control functions and interworking in next-generation networks (NGNs).
PGW_TimesTen	The Cisco PGW (Protocol Gateway) multi-protocol, carrier-grade soft-switch described above but with TimesTen capability.
Technician Server	A generic form of server. This is a general purpose server product that is capable of assuming multiple roles.
UnmanagedPBX	Unmanaged PBXs are often used as parent components for a location.

IP PBX Server

For the tools that are accessible from the Manage PBX Server screen, see [PBX Server Management on page 322](#).

An IP-PBX provides the core call processing application that is the foundation of an end-to-end IPT architecture. It provides signaling and call control services and provides all the call feature capabilities for users of the service.

Note

You must be a Service Provider Administrator, or higher, to access IP PBX features.

Procedure

Adding an IP PBX Server

To add a server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Add** button.
- Step 3** Select the required server type.
- Step 4** Complete the required fields and click the **Add** button. The server is added to the system.
-

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a CCM Server on page 116](#)
- [Adding an Unmanaged PBX Device\(s\) on page 156](#)

Procedure

Modifying an IP PBX Server

To modify a PBX Device:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button. The server is updated with the changes.
-

Procedure

Deleting a PBX Server

To delete a server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the server is removed from the system.
-

DHCP Server Management

DHCP stands for Dynamic Host Configuration protocol and is responsible for managing the IP addresses for client devices running on a network. Importantly DHCP can assign IP addresses to a client phone from a pool of valid IP addresses, on a per subnet basis, rather than per host.

Common management tasks for DHCP servers include loading, testing and synchronizing the servers.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a DHCP Server

To add a server:

- Step 1** Browse to *Network > DHCP Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required sever type (For Cisco implementations this would be ISC).
 - Step 4** Complete the required fields and click the **Add** button.
-

The server is added to the system.

Procedure

Modifying a DHCP Server

To modify a DHCP Server:

- Step 1** Browse to *Network > DHCP Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting a DHCP Server

To delete a server:

- Step 1** Browse to *Network > DHCP Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > DHCP Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.

- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

TFTP Server Management

Note

When adding a TFTP enabled *Cisco Unified Communications Manager*, the TFTP server should automatically appear in the *TFTP server* section of the *Network* menu.

TFTP stands for Trivial File Transfer Protocol and defines the protocol for a basic file transfer. A TFTP Server is typically a Line Cisco Call Manager Publisher and provides the basic set-up and configuration files for IP devices, such as Phones, once they have received an IP address and are registered onto the Call Manager.

Note: You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a TFTP Server

To add a server:

- Step 1** Browse to *Network > TFTP Servers*.
- Step 2** Click the **Add** button.
- Step 3** Select the required sever type.
- Step 4** Complete the required fields and click the **Add** button.

The server is added to the system.

Procedure

Modifying a TFTP server

To modify a FTP Server:

- Step 1** Browse to *Network > TFTP Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The server is updated with the changes.

Deleting a TFTP server

To delete a server:

- Step 4** Browse to *Network > TFTP Servers*.
- Step 5** Select the *Name* (active text link) of the server that you would like to delete.
- Step 6** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Voicemail Gateway Management

Voicemail gateways enable existing voicemail systems(modern or legacy systems) to connect and interact with a Cisco IP telephony network.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

From the Voicemail Gateway Management page, a tool is accessible to connect a Voicemail Gateway to an IPPBX by selecting the **Voicemail Gateway - IPPBX** button: see [Voicemail Gateway/IPPBX Management on page 100](#).

Procedure

Adding a Voicemail Gateway

To add a gateway:

- Step 1** Browse to *Network > Voicemail Gateways*.
 - Step 2** Click the **Add** button.
 - Step 3** Complete the required fields and click the **Add** button.
-

The gateway is added to the system.

The following fields are available when adding a Voicemail gateway:

Field	Description
<i>Host Name</i>	Must be unique in the system. This is a mandatory field.
<i>IP Address</i>	The IP address of the server being added. The IP address must be unique within the system. This is a mandatory field.
<i>Email Address</i>	The email address of the person responsible for the server. This is a mandatory field.
<i>Description</i>	A short description of the server
<i>Role</i>	This field displays the role that the server fulfill, such as a DHCP Server. This field cannot be edited by users and is used for information purposes only.
<i>Voicemail Ports</i>	Select the number of ports that you would like this server to be capable of handling.

Procedure

Modifying a Voicemail Gateway

Follow these steps to modify a Voicemail Gateway

- Step 1** Browse to *Network > Voicemail Gateways*
- Step 2** Select the **Name** (active text link) of the gateway that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The gateway is updated with the changes.

Procedure

Deleting a Voicemail Gateway

Follow these steps to delete a gateway:

- Step 1** Browse to *Network > Voicemail Gateways*.
 - Step 2** Select the **Name** (active text link) of the gateway that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the gateway is removed from the system.

Procedure

Testing the Gateway

Follow these steps to test a gateway:

- Step 1** Browse to *Network > Voicemail Gateways*.
 - Step 2** Select the **Name** (active text link) of the gateway that you would like to test.
 - Step 3** Click the **Test** button.
-

The gateway is tested and the results displayed on screen.

VoiceMail Gateway/IPPBX Management

A Voicemail Gateway can be associated with an IPPBX(s).

Procedure

Viewing associated IPPBXs

To view IPPBXs currently associated to the selected Voicemail Gateway:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **VoiceMail Gateway==>IPPBX** button adjacent to the Voicemail Gateway that you would like to view.

A screen is displayed, with two columns, one listing the registered (and available) IPPBXs, and the other displaying the IPPBXs current connection status. If the button adjacent to the IPPBX says **Connect**, the IPPBX is available for connection. If the button says **Disconnect**, the IPPBX is already connected.

Procedure

Associating (connecting) a Voicemail Gateway to an IPPBX

To associate a Voicemail Gateway to a IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.

- Step 2** Click the **Voicemail Gateway==>IPPBX** button adjacent to the Voicemail Gateway that you would like to associate.
- Step 3** Click the **Connect** button Adjacent to the IPPBX that you would like to associate with the Voicemail Gateway.

The Voicemail Gateway is associated with the selected IPPBX.

Procedure

Disassociating (disconnecting) a Voicemail Gateway from an IPPBX

To disassociate a Voicemail Gateway from a IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Voicemail Gateway==>IPPBX** button adjacent to the Voicemail Gateway that you would like to disassociate from a IPPBX(s).
- Step 3** Click the **Disconnect** button Adjacent to the IPPBX that you would like to disassociate from the Voicemail Gateway.

The Voicemail Gateway is disassociated from the selected IPPBX.

IP Edge Device Management

An IP Edge Device is typically a Line Powered Switch (Cisco 2800/3500) that is installed in a Location. It is used to connect IP phones to the IP WAN through a local router.

Note: You must be at the Service Provider Administrator user level, or higher, to access this functionality.

From the IP Edge Device Management page, the following tools are accessible:

Task	Accessed Via	Description
<i>IP Edge device Modification</i>	Select the <i>Name</i> (active text link) of the device that you would like to modify.	For more information, see the Modifying an IP Edge Device section.
<i>Addition of new IP Edge devices</i>	Click the Add button.	For more information, see the Adding an IP Edge device section.

Procedure

Adding an IP Edge Device

To add an IP Edge Device:

- Step 1** Browse to *Network > IP Edge Device*.
- Step 2** Click the **Add** button.
- Step 3** Select the required server type.
- Step 4** Complete the required fields and click the **Add** button. The following fields are available:

Field	Description	Remarks
Host Name	Must be unique in the system.	This is a mandatory field.

Field	Description	Remarks
Email Address	The email address of the person responsible for the server.	This is a mandatory field.
Description	A short description of the server.	-
Role	This field displays the role that the server fulfills, such as a DHCP Server.	This field cannot be edited by users and is used for information purposes only.

The IP edge device is added to the system.

Procedure

Modifying an IP Edge Device

To modify an IP Edge Device:

- Step 1** Browse to *Network > IP Edge Device*.
- Step 2** Select the *Name* (active text link) of the IP Edge Device that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The IP Edge Device is updated with the changes.

Procedure

Deleting an IP Edge Device

To delete an IP Edge Device:

- Step 1** Browse to *Network > IP Edge Device*.
- Step 2** Select the *Name* (active text link) of the IP Edge Device that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the IP Edge Device is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > IP Edge Device*.
- Step 2** Select the *Name* (active text link) of the IP Edge Device that you would like to test.
- Step 3** Click the **Test** button.

The IP Edge Device is tested and the results displayed on screen.

Console Servers and Services

This section covers the management of Console servers and services.

Operator Console Management

Console Servers provide a secure way of accessing network equipment in the event of an outage. Console servers are also a powerful tool for monitoring and managing multiple network devices dispersed over a wide area.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a Console Server

To add a server:

- Step 1** Browse to *Network > Console Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button.
-

The server is added to the system.

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a CCM Server on page 116](#)
- [Add a Netwise Cluster on page 178](#)

Procedure

Modifying a Console Server

To modify a Console Server:

- Step 1** Browse to *Network > Console Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting a Console Server

To delete a server:

- Step 1** Browse to *Network > Console Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Console Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to test.
 - Step 3** Click the **Test** button.
-

The server is tested and the results displayed on screen.

Console Service Management

The Console Services page enables administrators to enable and configure console access for a location. This can assist greatly with managing and administering locations.

Important

Before adding a console service, please ensure that a Console Server has been added to the system.

Adding a Console Service

Procedure

Adding a Console Service

To add a console service:

- Step 1** Browse to *Resources > Console Services*.
 - Step 2** Click the **Add** button.
 - Step 3** Complete the required fields and click the **Add** button.
-

The Console Service is added to the system.

The available fields include:

Field	Description
Name	The name of the console service being added. This is a mandatory field.
Description	A short description of the Console Service being added.
Country	The country within which the console service is operating. This is a mandatory field.
Hardware Group	This is the hardware group within which the Console Service resides. This is a mandatory field and a hardware group must be selected.

View and Modify a Console Service

Procedure

Viewing Console Services

To view a console service:

- Step 1** Browse to *Resources > Console Services*.
- Step 2** Select the *Name* (active text link) of the Console Service that you would like to view.

The details of the selected Console Service are displayed.

Procedure**Deleting a Console Service**

To delete a console service:

- Step 1** Browse to *Resources > Console Services*.
- Step 2** Select the *Name* (active text link) of the Console Service that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the delete operation, the Console Service is deleted from the system.

Procedure**Assigning a Console Service to a Location**

To assign a console service to a location:

- Step 1** Browse to *Resources > Console Services*.
- Step 2** Select the *Name* (active text link) of the Console Service that you would like to assign to a location.
- Step 3** Click the **Assign to Location** button.
- Step 4** Select the required location from the drop-down list.
- Step 5** Click the **Assign Location** button.

The Console Service is assigned to the location.

Music Server Management

A Music, or Music on Hold (MOH), server is an application that provides music on hold audio sources and connects a music on hold audio source to a number of different streams. The MOH server is used by the Cisco CallManager Music On Hold feature to provide users with music while they are on hold.

Note

- You must be at the Service Provider Administrator user level, or higher, to access this functionality.
 - When adding a Music on Hold (MOH) enabled *Cisco Unified Communications Manager*, the MoH server should automatically appear in the *Music Servers* section of the system's *Network* menu.
-

Procedure

Adding a Music on Hold (MoH) Server(s)

To add a MoH server:

- Step 1** Browse to *Network > Music Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button. The server is added to the system.
-

For information on available fields, see [Available Server Fields on page 919](#) if required.

Procedure

Modifying a Music Server

To modify a Music Server:

- Step 1** Browse to *Network > Music Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting a Music Server

To delete a server

- Step 1** Browse to *Network > Music Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Music Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to test.
 - Step 3** Click the **Test** button.
-

The server is tested and the results displayed on screen.

SMTP Server Management

The SMTP server that is used to forward voicemail messages to devices that support SMTP is managed on the *SMTP Server Management* page. A SMTP server can be added, modified and deleted.

Procedure

Add a SMTP server

To add a SMTP server:

Step 1 Enter the values in the input fields on the *Add SMTP Server* page as required.

The following fields are available when adding a SMTP server:

Field	Description
<i>Hostname</i>	The IP address or DSN name of the SMTP server. This is a mandatory field.
<i>Port</i>	The TCP port number for the SMTP server (typically 25). This is a mandatory field.
<i>Username</i>	Account Name on the SMTP server (if the server requires authentication)
<i>Password</i>	Account Password on the SMTP server (if server requires authentication).
<i>From address</i>	The email address from which the emails will be sent. This is a mandatory field.
<i>SMTP Auth</i>	Select the SMTP authentication type used by the SMTP server from the drop-down box. The available authentication types are: <ul style="list-style-type: none"> • <i>None</i> • <i>Basic Auth</i> • <i>TLS/STARTTLS</i> • <i>SSL</i>

Step 2 Click the **Add** button.

The SMTP server is added.

Procedure

Modifying a SMTP server

Step 1 Modify the selected values of the fields. Refer to the table of fields and values when adding a SMTP server.

Step 2 Click the **Modify** button.

The details of the SMTP server are modified.

Procedure

Delete a SMTP server

- Click the **Delete** button.

The SMTP server is removed.

Conference Server Management

A Conference server is a software/hardware combination that enables participants to engage in real-time conference calls. The server often provides all of the control and data management facilities for the conference calls and often provides the ability to control the entering and departure of participants from calls.

The system supports a number of conference servers, such as WebEx. Hence, it is possible to have a standalone conference server that is not necessarily a Call Manager.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a Conference Server(s)**Note**

To fully deploy a conference server, you must first add the server then associate it with a CCM.

To add a conference server:

- Step 1** Browse to *Network > Conference Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button. The server is added to the system.
-

For information on available fields, see [Available Server Fields on page 919](#) if required.

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a CCM Server on page 116](#)
- [Add an IP Unity Server on page 119](#)
- [Provisioning WebEx on page 633](#)

Procedure

Modifying a Conference Server

To modify a Conference Server:

- Step 1** Browse to *Network > Conference Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.

- Step 3** Modify the required fields and click the **Modify** button.

The server is updated with the changes.

Procedure

Deleting a Conference Server

To delete a server:

- Step 1** Browse to *Network > Conference Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Conference Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.
- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

Procedure

Associate a CCM Cluster with the Conference Server

To associate a CCM with a conference server:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Click the **Connectivity** button adjacent to the CCM that you would like to associate.
- Step 3** Click the **PBX=>Conference** button.
- Step 4** Click the **Connect** button adjacent to the conference server that you would like to associate the CCM to. The CCM is associated to the conference server.

Conference/Transit Server Management

A Conference Server can be associated with a Transit Server(s).

Note: Connecting a WebEx server to a transit server is not applicable.

Procedure

Viewing associated Transit Servers

To view Transit Servers currently associated to the selected Conference Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **Conference Server ==> Transit** button adjacent to the Conference Server that you would like to view

A screen is displayed, with two columns, one listing the registered (and available) Transit Servers, and the other displaying the Transit Servers current connection status. If the button adjacent to the Transit Server says **Connect**, the Transit Server is available for connection. If the button says **Disconnect**, the Transit Server is already connected.

Procedure

Associating (connecting) a Conference Server to a Transit Server

To associate a Conference Server to a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **Conference Server ==> Transit** button adjacent to the Conference Server that you would like to associate.
- Step 3** Select the **Connect** button Adjacent to the Transit Server that you would like to associate with the Conference Server.
-

The Conference Server is associated with the selected Transit Server.

Procedure

Disassociating (disconnecting) a Conference Server from a Transit Server

To disassociate a Conference Server from a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **Conference Server ==> Transit** button adjacent to the Conference Server that you would like to disassociate from a Transit Server(s).
- Step 3** Select the **Disconnect** button Adjacent to the Transit Server that you would like to disassociate from the Conference Server.
-

The Conference Server is disassociated from the selected Transit Server.

Modify and Delete a Contact Center Server

Procedure

To modify a Contact Center Server:

- Step 1** Browse to *Network > Contact Center Servers* .
- Step 2** Select the required *Contact Center* (active text link).
- Step 3** Make the required modifications, and then click the Modify button.
-

Procedure

To delete a Contact Center Server:

- Step 1** Browse to *Network > Contact Center Servers* Server.
- Step 2** Select the required Contact Center *Server* (active text link).
- Step 3** Click the Delete button to remove the Contact Center Server.

Procedure

Connecting a Contact Center Server to PBX/Transit

This feature allows a user to connect a Contact Center Server to the PBX/Transit.

This functionality is accessed by browsing to *Network > Contact Center Servers*.

Note

- The Route List: RL-UCCE-CVP-OR-CUBESP-#CCCPID#, (where #CCCPID# is the CPID of the Contact Center Server) must be manually added to the Unified CM before connecting the Contact Center to IPPBX.
- The Device Pool: GL-DP-CC must be manually added to the Unified CM before connecting the Contact Center to the IPPBX.
- The Route List and Device Pool names are customized as per the 01 Leaf Cluster Model workbook.
- Once a Contact Center has been created there are two ways it can be connected to a PBX/Transit device:

- Step 1 Scenario 1:**
- a Browse to *Network > Contact Center Servers* Server.
 - b Click the Connectivity button next to the relevant Contact Center Server.
 - c Click the **Connect** or Disconnect button next to the PBX/Transit to connect/disconnect this Contact Center Server.
- Step 2 Scenario 2:**
- a Browse to *Network > PBX Devices* .
 - b Click the Connectivity button next to the PBX to connect a Contact Center Server.
 - c Click the PBX=>Contact Center button.
 - d Click the **Connect** or Disconnect button next to the PBX/Transit to connect/disconnect the Contact Center Server.

Transcoder Server Management

Transcoder Servers enable the use of multiple protocols simultaneously within the system. Transcoders also enable administrators to expand the selection of protocols supported by the system.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Note

To fully deploy a server, you must first add the server then associate it with a CCM.

Procedure

Adding a Transcoder Server(s)

To add a transcoder server:

- Step 1** Browse to *Network > Transcoder Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button. The server is added to the system.
-

For information on available fields, see [Available Server Fields on page 919](#) if required.

Procedure

Modifying a Transcoder Server

To modify a Transcoder Server:

- Step 1** Browse to *Network > Transcoder Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting a Transcoder Server

To delete a server:

- Step 1** Browse to *Network > Transcoder Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Transcoder Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.

- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

Associate a CCM Cluster with the Transcoder Server

Procedure

To associate a CCM with a transcoder server:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Click the **Connectivity** button adjacent to the CCM that you would like to associate.
- Step 3** Click the **PBX=>Transcoder** button.
- Step 4** Click the **Connect** button adjacent to the transcoder server that you would like to associate the CCM to. The CCM is associated to the transcoder server.
-

Annunciator Server Management

The following functionality is available via the Annunciator Server section:

- [Selecting the Server Type to Add on page 94](#)
- **CCM Server**

[Add a CCM Server on page 116](#)

[CCM Cluster Management on page 125](#)

- **Technician Server**

[Add a Technician Server on page 115](#)

[Manage Generic Server on page 115](#)

Annunciator Servers are used to supply streams of either tones or announcements. Tones and announcements are considered the same as far as the annunciator is concerned.

When used in a cluster format, all annunciators in the cluster contain the same audio files. This enables CallManager to allocate an annunciator from any server that is available to play either a tone or an announcement. Annunciators can be connected to IP phones, gateways, MTPs, conference bridges, and other devices to inject either audio announcements or tones as required.

Announcements can be localized, allowing them to be used in different countries and locales. When a locale is installed on CallManager, the announcements and tones are associated with that locale. Two types of locales are available:

- User locale
- Network locale

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding an Annunciator Server

To add a server:

- Step 1** Browse to *Network > Annunciator Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button.
-

The server is added to the system.

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a CCM Server on page 116](#)

Procedure

Modifying an Annunciator

To modify an Annunciator Server:

- Step 1** Browse to *Network > Annunciator Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting an Annunciator

To delete a server:

- Step 1** Browse to *Network > Annunciator Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Annunciator Servers*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.
- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

Add a Technician Server

Procedure

To add a Technician Server:

- Step 1** Browse to the relevant sub-menu under the Network menu.
- Step 2** Click the **Add** button.
- Step 3** If asked to specify what type of Server you would like to add, click the **Add** button adjacent to Technician Server. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and click the **Add** button.

The Technician server is added to the system.

Note

Depending on the configuration of your system, some of these fields may not be available.

The following fields are available when adding a Technician Server:

Field	Description
Host Name	Must be unique in the system. This is a mandatory field.
IP Address	The IP address of the server being added. The IP address must be unique within the system. This is a mandatory field.
Email Address	The email address of the person responsible for the server. This is a mandatory field.
Description	A short description of the server
Role	This field displays the role that the server fulfills, such as a DHCP Server. This field cannot be edited by users and is used for information purposes only.
Transit Switch code (CPID)	Select from the drop-down list the required Transit Switch code (CPID).

Manage Generic Server

Procedure

To manage a Generic Server:

- Step 1** Browse to *Network > IP Edge Devices*.
- Step 2** Select the relevant Technician server *Name* (active text link) that you would like to modify. The *Manage Generic Server* screen is displayed.
- Step 3** Modify the required fields. The following fields are available when modifying a Technician Server.

Note: Depending on the configuration of your system, some of these fields may not be available

Field	Description
Server Name	Must be unique in the system. This is a read-only field and cannot be modified here.
Description	A short description of the server/
Service Status	Select the required service status from the drop-down list. Options include, <i>In Service</i> , <i>Not in Service</i> , and <i>Out of Service</i> .
Email Address	The email address of the person responsible for the server. This is a mandatory field.
IP Edge Device	Indicates whether the server is being used as an IP Edge Device (Y or N).

- Step 4** Click the **Modify** button when complete. The server details are updated in the system.

Procedure

Deleting a Generic Server

To delete a Generic Server:

- Step 1** Browse to *Network > IP Edge Devices*.
- Step 2** Select the relevant Technician server *Name* (active text link) that you would like to delete. The *Manage Generic Server* screen is displayed.
- Step 3** Click the **Delete** button. The server is deleted from the system.

Note: Depending on the configuration of your system, confirmation may be requested prior to deleting a server.

Technician Server Tools

Server Tools enable administrators to perform advanced operations on Technician Servers. For more information on available tools, please consult the relevant Feature Guide.

Add a CCM Server

Procedure

To add a CCM Server:

- Step 1** Browse to the relevant sub-menu under the Network menu.
- Step 2** Click the **Add** button.
- Step 3** If asked to specify what type of Server you would like to add, click the **Add** button adjacent to CCM Server. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and click the **Add** button. The CCM server is added to the system.

Note

Depending on the configuration of your system, some of these fields may not be available.

The following fields are available when adding a CCM Server:

Field	Description
Software Version	<p>Select the software version that the server is running. For example, CCM : 8.6.x or CCM : 9.0.x. This is a mandatory field.</p> <p>Only supported versions are shown on the list. Clusters with an unsupported version will show an error message (Software Version [CCM : {version number}] is no longer supported) and the version will default to the lowest version available.</p>
Label	The label (name) of the server. This server label must be unique in the system. This is a mandatory field.
Description	A short description of the server.
Publisher Host Name	<p>Hostname for the server where the Unified Communications Manager is installed. This is a mandatory field.</p> <p>Note</p> <p>This should be the actual hostname of the server.</p>
Publisher CCM Name	CCM name for the server where the Unified CM is installed. This is a mandatory field. Note: This should be the name of the server as shown in Unified CM (typically the IP Address of the server). This can be found via <i>System > Cisco Unified CM</i> .
Publisher IP Address	This is the IP address used by CUCDM when communicating with the Unified CM server. This is only true for the publisher. This is also the address that is used to create trunks (publisher and subscribers) between PBXs. This is a mandatory field.
Publisher IP Address B	This IP address is available for use by Gateways when communicating with the Unified CM server. A Gateway option allows the user to specify whether the normal IP Address or this address is used. This allows support for various NAT configurations. See the IOS Gateways Guide for details on how to use these settings/options.
Publisher Config User-name	The user name for configuring the server. This is a mandatory field.
Publisher Config Password	<p>The password to be used when configuring the server. This is a mandatory field.</p> <p>Note</p> <p>Due to a known issue with the Unified CM password algorithm, ensure that you do not include the "@" symbol in the password. Unified CM does not handle passwords containing the "@" symbol correctly.</p>
Domain Name	<p>The value entered in this field is used to apply a new domain name to all registered Cisco Dual Mode for Android devices.</p> <p>Important</p> <p>To apply the domain name to devices, the Operations Tool Apply Domain Name to Android devices must be run.</p> <p>Note</p> <p>The field is limited to 50 alphanumeric characters in length, including these punctuation symbols: space, period, hyphen and underscore.</p>

Field	Description
Country	Select the country within which the server is situated from the drop-down list. This is a mandatory field.
Annunciator Server	Select this checkbox if the server is going to be used as an Annunciator server.
Conference server	Select this checkbox if the server is going to be used as a Conference server.
EMCC server	Select this checkbox if the server is going to be used as a EMCC server.
IP PBX	Select this checkbox if the server is going to be used as an IP PBX. This is a mandatory field.
Max. IPPBX lines per device	If you have selected the IP PBX checkbox, use this field to specify the maximum number of IPPBX Lines that are available for use by each device.
Media Termination Point	Select this checkbox if the server is going to be used as a Media Termination Point.
Music server	Select this checkbox if the server is going to be used as a Music Server.
Switchboard/Console server	Select this checkbox if the server is going to be used as a Switchboard/Console server.
TFTP server	Select this checkbox if the server is going to be used as a TFTP server.
CPID	If you would like the system to automatically select the required value, select the Auto option, alternatively, select the required value from the drop-down list. This is a mandatory field.
ClusterID	If you would like the system to automatically select the required value, select the Auto option, alternatively, select the required value from the drop-down list. This is a mandatory field.
Call Processor Engine	Select this checkbox if required to enable the call processor engine.
Manual Configuration Mode (Use for Un-Managed Clusters)	Select this checkbox if you would like the server to operate in manual configuration mode. This option should be selected for un-managed clusters. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that is used for manual activation of the CCM Server. This field is mandatory if the Manual Configuration Mode? option has been selected.
Service Status	Select the required service status from the drop-down list, namely <i>In Service</i> , <i>Not In Service</i> or <i>Out of service (maintenance)</i> .
Minimum AXL Interaction Time	Select the required option from the drop-down list, options include <i>0.1 Second</i> , <i>0.4 Second</i> , <i>0.8 Second</i> and <i>1.2 Seconds</i> .
Network Monitoring active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note</p> <p>Depending on network loads, selecting this option may impact on the performance of the server.</p>
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.

Field	Description
Encrypt configuration sessions?	<p>Select this option if you would like all configuration sessions with the server to be encrypted.</p> <p>Note</p> <p>While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.</p>
LDAP Aware?	If the LDAP Aware option is checked, the CCM is in a "semi-manual" mode in terms of adding users. When a user is added, the system performs a check on these devices to ensure that the user does indeed exist on the device.

Add an IP Unity Server

Procedure

To add an IP Unity Server:

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Add** button
- Step 3** If asked to specify what type of Server you would like to add, select the **Add** button adjacent to *IP Unity Server*. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and select the **Add** button

The IP Unity server will be added to the system.

The following fields are available when adding an IP Unity Server:

Note: Depending on the configuration of your system, some of these fields may not be available.

Field	Description
<i>Host Name</i>	Host name for the server. Must be unique in the system. This is a mandatory field.
<i>IP Address</i>	IP Address for the server This is a mandatory field.
<i>Description</i>	A short description of the server.
<i>Config User Name</i>	The user name for configuring the server. This is a mandatory field.
<i>Config Password</i>	The password to be used when configuring the server. This is a mandatory field.
<i>Software Version</i>	Select the software version that the server will be running, alternatively, you can select the Any option. This is a mandatory field.
<i>Call Back IP Address for API Response</i>	The IP address that will be used for Call Backs during API Response. This is a mandatory field.
<i>Maximum Number of Participants For All parallel reserved conferences</i>	The maximum number of participants that will be allowed to participate in reserved conferences at any one time. This is a mandatory field.
<i>Maximum Number of Participants For All parallel Ad hoc conferences</i>	The maximum number of participants that will be allowed to participate in ad hoc conferences at any one time. This is a mandatory field.

Field	Description
<i>Maximum Number of Participants per Reserved conference</i>	The maximum number of participants that will be allowed to participate in a single reserved conference. This is a mandatory field.
<i>Maximum Number of Participants per Ad hoc conference</i>	The maximum number of participants that will be allowed to participate in a single ad hoc conference. This is a mandatory field.
<i>PGW RTLIST used for SIP Trunk</i>	The PGW RTLIST that will be used for the SIP Trunk
<i>CPID</i>	If you would like the system to automatically select the required value, select the Any option, alternatively, select the required value from the drop-down list. This is a mandatory field.
<i>Manual Configuration Mode?</i>	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
<i>Email address for Manual activation</i>	The email address that will be used for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
<i>Network Monitoring active?</i>	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
<i>Detailed trace file of configuration sessions ?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Conference server</i>	Select this checkbox if the server is going to be used as a Conference server.
<i>IVR server</i>	Select this checkbox if the server is going to be used as an IVR server.
<i>Voicemail server</i>	Select this checkbox if the server is going to be used as a Voicemail server.

View and Modify an IP Unity Server

From the View and Modify an IP Unity Server page, the following tools are accessible:

Tool/Task	Accessed Via	Description
<i>Test</i>	Select the Test button.	A test of the server will occur immediately and the results of the test will be displayed.
<i>Server Modification</i>	Make the required changes and select the Modify button.	For more information, see the Modify section below.
<i>Delete</i>	Select the Delete button.	This will delete the server from your system. Important: Depending on the configuration of your system, confirmation may be requested prior to deleting a server.
<i>Manage IPUnity Conference Class of Service</i>	Select the Manage Conference Class of Service button.	For more information, see View and Modify an IP Unity Server's Class of Service on page 123.

Procedure

Modifying an IP Unity Server

To modify an IP Unity server:

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity server that you would like to modify.
- Step 3** Modify the required fields and select the **Modify** button

The IP Unity server will be modified within the system.

The following fields are available when modifying an IP Unity server:

Note: Depending on the configuration of your system, some of these fields may not be available

Field	Description
<i>Host Name</i>	Hostname for the server. Must be unique in the system. This is a mandatory field.
<i>IP Address</i>	IP Address for the server This is a mandatory field.
<i>Description</i>	A short description of the server.
<i>Config User Name</i>	The user name for configuring the server. This is a mandatory field.
<i>Config Password</i>	The password to be used when configuring the server. This is a mandatory field.
<i>Software Version</i>	Select the software version that the server will be running, alternatively, you can select the Any option. This is a mandatory field.
<i>Call Back IP Address for API Response</i>	The IP address that will be used for Call Backs during API Response. This is a mandatory field.
<i>Maximum Number of Participants For All parallel reserved conferences</i>	The maximum number of participants that will be allowed to participate in reserved conferences at any one time. This is a mandatory field.
<i>Maximum Number of Participants For All parallel Ad hoc conferences</i>	The maximum number of participants that will be allowed to participate in ad hoc conferences at any one time. This is a mandatory field.
<i>Maximum Number of Participants per Reserved conference</i>	The maximum number of participants that will be allowed to participate in a single reserved conference. This is a mandatory field.
<i>Maximum Number of Participants per Ad hoc conference</i>	The maximum number of participants that will be allowed to participate in a single ad hoc conference. This is a mandatory field.
<i>PGW RTLIST used for SIP Trunk</i>	The PGW RTLIST that will be used for the SIP Trunk
<i>CPID</i>	If you would like the system to automatically select the required value, select the Any option, alternatively, select the required value from the drop-down list. This is a mandatory field.
<i>Manual Configuration Mode?</i>	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
<i>Email address for Manual activation</i>	The email address that will be used for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.

Field	Description
<i>Network Monitoring active?</i>	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
<i>Detailed trace file of configuration sessions ?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Conference server</i>	Select this checkbox if the server is going to be used as a Conference server.
<i>IVR server</i>	Select this checkbox if the server is going to be used as an IVR server.
<i>Voicemail server</i>	Select this checkbox if the server is going to be used as a Voicemail server.

Procedure

Managing the Servers Class of Service

To manage the servers class of service:

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity server that you would like to modify.
- Step 3** Select the **Class of Service** button

A screen will open enabling you to manage the servers class of service.

Manage an IP Unity Server's Class of Service

Procedure

Adding a Class of Service

To add class of service to an IPunity server:

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity Server that you would like to modify.
- Step 3** Select the **Class of Service** button
- Step 4** Complete the required fields and select the **Add** button.

The class of service will be added for the server.

Available fields include:

Field	Description
<i>Name</i>	Specify a name for the class of service. This is a mandatory field.
<i>Address Book Upload</i>	Select this checkbox if you would like to include Address Book Upload in the class of service.
<i>Blast Dial</i>	Select this checkbox if you would like to include Blast Dial in the class of service.
<i>Conference Voting</i>	Select this checkbox if you would like to include Conference Voting in the class of service.

Field	Description
<i>Consultative OutCall</i>	Select this checkbox if you would like to include Consultative OutCall in the class of service.
<i>Data Collaboration</i>	Select this checkbox if you would like to include Data Collaboration in the class of service.
<i>DNIS</i>	Select this checkbox if you would like to include DNIS in the class of service.
<i>Name Recording</i>	Select this checkbox if you would like to include Name Recording in the class of service.
<i>Operator Support</i>	Select this checkbox if you would like to include Operator Support in the class of service.
<i>OutCall</i>	Select this checkbox if you would like to include OutCall in the class of service.
<i>Outlook Integration</i>	Select this checkbox if you would like to include Outlook Integration in the class of service.
<i>Talk Indicator</i>	Select this checkbox if you would like to include Talk Indicator in the class of service.

Procedure

Modifying a Class of Service

To manage an IPunity server's class of service, follow these steps

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity Server that you would like to modify.
- Step 3** Select the **Class of Service** button
- Step 4** Select the **Name** (active text link) of the Class of Service that you would like to modify
- Step 5** Modify the required fields and select the **Modify** button

The class of service will be modified within the system.

Procedure

Deleting a Class of Service

To delete an IPunity server's class of service, follow these steps

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity Server that you would like to modify.
- Step 3** Select the **Class of Service** button
- Step 4** Select the **Name** (active text link) of the Class of Service that you would like to delete
- Step 5** Select the **Delete** button

After confirming the operation, the class of service will be deleted from the system.

View and Modify an IP Unity Server's Class of Service

Procedure

Modifying a Class of Service

To manage an IPunity server's class of service, follow these steps

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity Server that you would like to modify.
- Step 3** Select the **Class of Service** button
- Step 4** Select the **Name** (active text link) of the Class of Service that you would like to modify
- Step 5** Modify the required fields and select the **Modify** button

The class of service will be modified within the system.

Available fields include:

Field	Description
<i>Name</i>	Specify a name for the class of service. This is a mandatory field.
<i>Address Book Upload</i>	Select this checkbox if you would like to include Address Book Upload in the class of service.
<i>Blast Dial</i>	Select this checkbox if you would like to include Blast Dial in the class of service.
<i>Conference Voting</i>	Select this checkbox if you would like to include Conference Voting in the class of service.
<i>Consultative OutCall</i>	Select this checkbox if you would like to include Consultative OutCall in the class of service.
<i>Data Collaboration</i>	Select this checkbox if you would like to include Data Collaboration in the class of service.
<i>DNIS</i>	Select this checkbox if you would like to include DNIS in the class of service.
<i>Name Recording</i>	Select this checkbox if you would like to include Name Recording in the class of service.
<i>Operator Support</i>	Select this checkbox if you would like to include Operator Support in the class of service.
<i>OutCall</i>	Select this checkbox if you would like to include OutCall in the class of service.
<i>Talk Indicator</i>	Select this checkbox if you would like to include Talk Indicator in the class of service.

Procedure**Deleting a Class of Service**

To delete an IPunity server's class of service, follow these steps

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the **Name** (active text link) of the IP Unity Server that you would like to modify.
- Step 3** Select the **Class of Service** button
- Step 4** Select the **Name** (active text link) of the Class of Service that you would like to delete
- Step 5** Select the **Delete** button

After confirming the operation, the class of service will be deleted from the system.

CCM Cluster Management

From the *CCM Cluster Management* screen, you can modify and delete the cluster as well as access functionality such as Servers, Groups, Attributes, View CCM Config, Media Services, Import Refresh Items, SIP Normalization Scripts, EMCC, and Trunk Config. To access any of the above functionality, click the appropriate button.

Note: Depending on the configuration of the selected cluster, certain buttons may not be available.

The following buttons are accessible from the CCM Cluster Management page:

Button	Accessed By	Description
<i>Modify</i>	Clicking the Modify button.	To modify a clusters configuration, make the required changes then click the Modify button.
<i>Load Static Config</i>	Clicking the Load Static Config button.	This option loads static configuration variables for the cluster. Important: There is no confirmation before the static config is loaded.
<i>Delete</i>	Clicking the Delete button.	This option deletes the CCM Server Cluster from the system. Important: Depending on the configuration of your system, confirmation is required when deleting an IOS device.
<i>Servers</i>	Clicking the Servers button.	For further information, see CCM Server Management on page 81
<i>Groups</i>	Clicking the Groups button.	For further information, see Unified CM Group Management on page 82
<i>Attributes</i>	Clicking the Attributes button.	For further information, see Cluster Management - Attribute Management on page 83
<i>View CCM Config</i>	Clicking the View CCM Config button.	For further information, see CCM Server Configuration on page 94
<i>Media Services</i>	Clicking the Media Services button.	For further information, see Media Services Management on page 87
<i>Import/Refresh Items</i>	Clicking the Import/Refresh Items button.	For further information, see Importing/Refreshing CCM Items on page 87
<i>SIP Normalization Scripts</i>	Clicking the SIP Normalization Scripts button.	For further information, see SIP Normalization Scripts Management on page 180
<i>EMCC</i>	Clicking the EMCC button.	For further information, see Extension Mobility Cross Cluster (EMCC) Configuration on page 401
<i>IP Phone Services</i>	Clicking the IP Phone Services button.	For further information, see Managing Phone Services on page 378

Button	Accessed By	Description
<i>Bandwidth Groups</i>	Clicking the Bandwidth Groups button.	For further information, see Bandwidth Groups on page 84
<i>Device Pool Templates</i>	Clicking the Device Pool Templates button.	For further information, see Device Pool Templates on page 558
<i>Audio Regions</i>	Clicking the Audio Regions button.	For further information, see Audio Regions on page 647
<i>Service Profiles</i>	Clicking the Service Profiles button.	For further information, see Service Profile Management on page 610

Procedure

Modifying a CCM server

To modify a CCM Server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM Server that you would like to modify.
- Step 3** **Note:** Depending on the configuration of your system, some of these fields may not be available

Modify the required fields. The following fields are available when modifying a CCM Server:

Field	Description
Name	The name of the server. This server label must be unique in the system. This is a mandatory field.
Static Config Loaded	The version of the loaded static config. For example, <i>2010-07-12 07:58:40.898554</i> . This field cannot be modified.
Cluster ID	If you would like the system to automatically select the required value, select the <i>Auto</i> option, alternatively, select the required value from the drop-down list. This is a mandatory field.
CPID	If you would like the system to automatically select the required value, select the <i>Auto</i> option, alternatively, select the required value from the drop-down list. This is a mandatory field.
Country	Select the country within which the server is situated from the drop-down list. This is a mandatory field but cannot be edited on this page.
Description	An optional description of the CCM cluster.
Config User ID	The user name for configuring the server.
Config Password	The password to be used when configuring the server. Important: Due to a known issue with the Unified CM password algorithm, please ensure that you do not include the "@" symbol in the password. Unified CM does not handle passwords containing the "@" symbol correctly.
Domain Name	The value entered in this field is used to apply a new domain name to all registered Cisco Dual Mode for Android devices. Important: To apply the domain name to devices, the Operations Tool <i>Apply Domain Name to Android devices</i> must be run. Note: The field is limited to 50 alphanumeric characters in length, including these punctuation symbols: space, period, hyphen and underscore.

Field	Description
Annunciator Server	Select this checkbox if the server is going to be used as an Annunciator server.
Conference server	Select this checkbox if the server is going to be used as a Conference server.
EMCC server	Select this checkbox to enable the server to be EMCC capable.
IP PBX	Select this checkbox if the server is going to be used as an IP PBX.
Max. IPPBX lines per device	If you have selected the <i>IP PBX</i> checkbox, use this field to specify the maximum number of IPPBX Lines that are available for use by each device.
Media Termination Point	Select this checkbox if the server is going to be used as a Media Termination Point.
Music server	Select this checkbox if the server is going to be used as a Music Server.
Switchboard/Console server	Select this checkbox if the server is going to be used as a Switchboard/Console server.
TFTP server	Select this checkbox if the server is going to be used as a TFTP server.
Software Version	<p>For example, CCM : 8.6.x or CCM : 9.0.x. This is a mandatory field.</p> <p>Only supported versions are shown on the list. Clusters with an unsupported version will show an error message (Software Version [CCM : {version number}] is no longer supported) and the version will default to the lowest version available.</p> <p>Note</p> <p>When the Unified CM is upgraded to a later version, and once the upgrade is complete, this field must be updated to reflect the new Unified CM version.</p>
Service Status	Select the required service status from the drop-down list. Options include, <i>In Service</i> , <i>Out of Service</i> and <i>Not in Service</i> .
Minimum AXL Interaction Time	Select the required minimum AXL Interaction time from the drop-down list. Options include <i>0.1</i> , <i>0.4</i> , <i>0.8</i> and <i>1.2</i> seconds.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. This option should be selected for un-managed clusters. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that is used for manual activation of the CCM Server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note: Depending on network loads, selecting this option may impact on the performance of the server.</p>
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	<p>Select this option if you would like all configuration sessions with the server to be encrypted.</p> <p>Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.</p>

Field	Description
LDAP Aware?	If the LDAP Aware option is checked, the CCM is in a "semi-manual" mode in terms of adding users. When a user is added, the system performs a check on these devices to ensure that the user does indeed exist on the device.

Step 4 Click the **Modify** button when complete. The CCM server is modified within the system.

Media Termination Point Management

Media Termination Points (MTP) are software-based or hardware-based media processing resources that accepts two full-duplex stream connections. They are used to bridge the media streams between the two connections and allow for the streaming connections to be setup and torn down independently. An MTP might also be used to perform other processing on a media stream, such as digit detection and insertion.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a Media Termination Point

To add a Media Termination Point server:

- Step 1** Browse to *Network > Media Termination Point*.
- Step 2** Click the **Add** button.
- Step 3** Select the required server type.
- Step 4** Complete the required fields and click the **Add** button.

The server is added to the system.

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a CCM Server on page 116](#)

Procedure

Modifying a Media Termination Point

To modify a Media Termination Point:

- Step 1** Browse to *Network > Media Termination Point*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The server is updated with the changes.

Procedure

Deleting a Media Termination Point

To delete a server:

- Step 1** Browse to *Network > Media Termination Point*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the *Delete* button.

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Media Termination Point*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.
- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

Directory Server Management

Directory servers are used to store your company's directory information in a logical structure that organizes user, group, and access information for easy retrieval and maintenance.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

Procedure

Adding a Directory Server

To add a server:

- Step 1** Browse to *Network > Directory Server*.
- Step 2** Click the **Add** button.
- Step 3** Select the required server type.
- Step 4** Complete the required fields and click the **Add** button.

The server is added to the system.

The following fields are available when adding a server:

Field	Description
Host Name	Must be unique in the system. This is a mandatory field.

Field	Description
IP Address	The IP address of the server being added. The IP address must be unique within the system. This is a mandatory field.
Email Address	The email address of the person responsible for the server. This is a mandatory field.
Description	A short description of the server
Role	This field displays the role that the server fulfills, such as a DHCP Server. This field cannot be edited by users and is used for information purposes only.

Procedure

Modifying a Directory Server

To modify a Directory server:

- Step 1** Browse to *Network > Directory Server*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The server is updated with the changes.

Procedure

Deleting a Directory Server

To delete a server:

- Step 1** Browse to *Network > Directory Server*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Directory Server*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.
- Step 3** Click the **Test** button.

The server is tested and the results displayed on screen.

Directory Service Management

To provide end-users with directory service functionality, a directory service needs to be defined.

Before adding a directory service, take note of the following:

- For a directory service to be offered at the Location level, they must be created at the Provider level and allocated to the Customers' Locations.
- Provider Administrators need to configure and manage directory service for each Customer and when new Locations are added.
- Before adding Directory Services, ensure that a Directory Server has been added to the location.

Add Directory Services

Before adding a directory service, please take note of the following:

- For a directory service to be offered at the Location level, they must be created at the Provider level and allocated to the Customers' Locations.
- Provider Administrators will need to configure and manage directory service for each Customer and when new Locations are added.
- Before adding Directory Services, please ensure that a Directory Server has been added to the location.

Procedure

Adding a Directory Service

To add a directory service:

- Step 1** Browse to *Resources > Directory Services*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields and click the **Add** button.

The Directory Service are added to the system.

The following fields are available when adding a new Directory Service:

Fields	Description
Name	The name to be used for the Directory server. This is a mandatory field.
Description	A short description for the Directory Service
Country	The country where the directory service will be located. This is a mandatory field.
Domain Name	The domain name where the Directory Service will reside.
Directory Server	The name of the directory server that the directory service will be utilizing. This is a mandatory field.

Viewing and Deleting Directory Services

Procedure

Viewing a Directory Service

You are able to view but not modify Directory Services, to view a Directory Service:

- Step 1** Browse to *Resources > Directory Services*.

- Step 2** Select the *Name* (active text link) of the Directory Service that you would like to view.
-

The details of the Directory Service are displayed.

The fields displayed include:

Fields	Description
Name	The name to be used for the Directory server. This is a mandatory field.
Description	A short description for the Directory Service
Country	The country where the directory service will be located. This is a mandatory field.
Domain Name	The domain name where the Directory Service will reside.
Directory Server	The name of the directory server that the directory service will be utilizing. This is a mandatory field.

Procedure

Deleting a Directory Service

To delete a directory service:

- Step 1** Browse to *Resources > Directory Services*.
- Step 2** Select the *Name* (active text link) of the Directory Service that you would like to delete.
- Step 3** Click the **Delete** button.
-

After confirming the deletion, the Directory Service is deleted from the system.

Emergency Responder Management

A Cisco Emergency Responder (CER) is part of the Enhanced 911 feature set that ensures an emergency service has a relevant call-back number for any phone that makes an emergency call. Where those extensions do not already have their own DDI capability, the Cisco Emergency Responder provides a temporary DDI. This temporary number is known as an ELIN (Emergency Location Id Number).

The system enables:

- Emergency responders to be configured and stores their individual characteristics in its database
- Locations to enable/disable emergency responder support

Note

- This functionality is a legal requirement in certain countries, please consult the relevant legislation for your region.
 - You must be at the Service Provider Administrator user level, or higher, to access this functionality.
-

Adding an Emergency Responder

Procedure

To add an Emergency Responder:

- Step 1** Browse to *Network > Emergency Responder*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the CiscoEmergencyResponder server type. The *Add Cisco Emergency Responder* screen is displayed.

Add Cisco Emergency Responder (Screen 1)

Procedure

- Step 1** Complete the required fields (see table below).
- Step 2** Click the **Next** button.

Field	Description
<i>Cisco Emergency Responder Group Name</i>	Must be unique in the system. This is a mandatory field.
<i>Cisco Emergency Responder Group Description</i>	A short description of the server. This is a mandatory field.
<i>ELIN of Default ERL (Format: code-number)</i>	Specify the ELIN of default ERL. This is a mandatory field.
<i>Peer TCP Port</i>	Specify the Peer TCP port number. This is a mandatory field.
<i>Heartbeat Count</i>	Specify the heartbeat count. This is a mandatory field.
<i>Heartbeat Interval (secs)</i>	Specify the heartbeat interval in seconds. This is a mandatory field.
<i>Active Call Timeout (mins)</i>	Specify the Active Call Timeout in minutes. This is a mandatory field.
<i>UDP Port Begin</i>	Specify the start of the UDP port range. This is a mandatory field.
<i>Software Version</i>	Select the version of server from the drop-down list.
<i>Country</i>	Select the country where the Cisco Emergency Responder will be situated. This is a mandatory field.
<i>Email address for Manual activation</i>	The email address that will be used for manual activation of the Server.
<i>Detailed trace file of configuration sessions?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Encrypt configuration sessions?</i>	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced based on the performance of your network.

Add Cisco Emergency Responder (Screen 2)

Procedure

- Step 1** Complete the required fields (see table below).

Step 2 Click the **Add** button.

The server is added to the system.

Note: Depending on the configuration of your system, some of these fields may not be available.

Field	Description
<i>Primary Cisco Emergency Responder Details</i>	
<i>Host Name</i>	Must be unique in the system. This is a mandatory field.
<i>Description</i>	A short description of the host name for the primary server.
<i>IP Address</i>	Specify the IP Address for the Primary Cisco Emergency Responder. This is a mandatory field.
<i>Config User Id</i>	This is an optional field when the server is configured in manual mode.
<i>Config Password</i>	This is an optional field when the server is configured in manual mode.
<i>Route Point for Main Server</i>	This is a mandatory field.
<i>Backup Cisco Emergency Responder Details</i>	
<i>Host Name</i>	Must be unique in the system. This is a mandatory field.
<i>Description</i>	A short description of the host name for the backup server.
<i>IP Address</i>	Specify the IP Address for the Backup Cisco Emergency Responder. This is a mandatory field.
<i>Config User Id</i>	This is an optional field when the server is configured in manual mode.
<i>Config Password</i>	This is an optional field when the server is configured in manual mode.
<i>Route Point for Backup Server</i>	This is a mandatory field.

Managing a Cisco Emergency Responder

Procedure

To modify an Emergency Responder:

- Step 1** Browse to *Network > Emergency Responder*.
- Step 2** Select the *Name* (active text link) of the server that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The following fields are available when modifying a Cisco Emergency Responder (CER) Server:

Note

Depending on the configuration of your system, some of these fields may not be available.

Field	Description
<i>Cisco Emergency Responder Group Name</i>	Must be unique in the system. This is a mandatory field.
<i>Cisco Emergency Responder Group Description</i>	A short description of the server. This is a mandatory field.

Field	Description
<i>ELIN of Default ERL (Format: code-number)</i>	<p>Note</p> <p>This field can not be modified when the CER is connected to the PBX.</p> <p>Specify the ELIN of default ERL. This is a mandatory field.</p>
<i>Peer TCP Port</i>	Specify the Peer TCP port number. This is a mandatory field.
<i>Heartbeat Count</i>	Specify the heartbeat count. This is a mandatory field.
<i>Heartbeat Interval (secs)</i>	Specify the heartbeat interval in seconds. This is a mandatory field.
<i>Active Call Timeout (mins)</i>	Specify the Active Call Timeout in minutes. This is a mandatory field.
<i>UDP Port Begin</i>	Specify the start of the UDP port range. This is a mandatory field.
<i>Software Version</i>	Select the version of server from the drop-down list.
<i>Country</i>	Select the country where the Cisco Emergency Responder will be situated. This is a mandatory field.
<i>Email address for Manual activation</i>	The email address that is used for manual activation of the Server.
<i>Detailed trace file of configuration sessions?</i>	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
<i>Encrypt configuration sessions?</i>	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.

Procedure

To delete a server:

- Step 1** Browse to *Network > Emergency Responder*.
- Step 2** Select the *Name* (active text link) of the server that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > Emergency Responder*.
- Step 2** Select the *Name* (active text link) of the server that you would like to test.
- Step 3** Click the **Test** button.

Cisco Emergency Responder Line Details

When connecting an IPPBX to an Emergency Responder Server, two fields must be completed:

Field	Description
<i>Telephony Port Begin Address</i>	Specify the port where you would like the first telephony address to be. This is a mandatory field.
<i>Number of Telephony ports required</i>	Specify the number of telephony ports that are required by the Cisco Emergency Responder. This is a mandatory field.

Once you have completed the above two fields, click the **Connect** button.

The connection between the IPPBX and the Cisco Emergency Responder Server is established.

Emergency Responder/IPPBX Server Management

An Emergency Responder Server can be associated with an IPPBX Server(s).

Procedure

Viewing associated IPPBX Servers

To view IPPBX Servers currently associated to the selected Emergency Responder Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the Emergency Responder Server that you would like to view connections for.
- Step 3** Click the **Emergency Responder==>PBX** button adjacent to the Emergency Responder Server that you would like to view

A screen is displayed, with two columns, one listing the registered (and available) IPPBX Servers, and the other displaying the IPPBX Servers current connection status. If the button adjacent to the IPPBX Server says **Connect**, the IPPBX Server is available for connection. If the button says **Disconnect**, the IPPBX Server is already connected.

Procedure

Associating (connecting) an Emergency Responder Server to an IPPBX Server

To associate a Emergency Responder Server to a IPPBX Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the Emergency Responder Server that you would like to view connections for.
- Step 3** Click the **Emergency Responder==>PBX** button adjacent to the Emergency Responder Server that you would like to associate.
- Step 4** Click the **Connect** button Adjacent to the IPPBX Server that you would like to associate with the Emergency Responder Server.
- Step 5** Enter the *Telephony Port Begin Address* and the *Number of Telephony ports* required, both fields are mandatory, and click the **Connect** button.

The Emergency Responder Server is associated with the selected IPPBX Server.

Procedure

Disassociating (disconnecting) an Emergency Responder Server from an IPPBX Server

To disassociate a Emergency Responder Server from a IPPBX Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the Emergency Responder Server that you would like to view connections for.
- Step 3** Click the **Emergency Responder==>PBX** button adjacent to the Emergency Responder Server that you would like to disassociate from a IPPBX Server(s).
- Step 4** Click the **Disconnect** button Adjacent to the IPPBX Server that you would like to disassociate from the Emergency Responder Server.

The Emergency Responder Server is disassociated from the selected IPPBX Server.

IVR Server Management

IVR Servers, also known as auto-attendant servers, provides the functionality to transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator. This is achieved via a system of voice menus that the person initiating the call interacts with via their telephone keypad or via voice commands.

Note

You must be at the Service Provider Administrator user level, or higher, to access this functionality.

From the IVR Server Management page, the following tools are accessible:

Task	Accessed Via	Description
<i>Adding an IVR Server</i>	Click the Add button.	For more information, see below.
<i>Connecting an IVR Server to a Transit switch</i>	Click the IVR Server => Transit button.	This page enables you to manage connections between an IVR Server and a Transit Switch. For more information, please see IVR/Transit Server Management on page 525 .
<i>IVR Server Modification</i>	Select the <i>Name</i> (active text link) of the IVR Server that you would like to modify.	For more information, see below.
<i>Associated Devices</i>	Select the <i>Associated Devices</i> active text link.	For more information, see Device Sets on page 347 .

Procedure

Adding an IVR Server

To add a server:

- Step 1** Browse to *Network > IVR Servers*.
 - Step 2** Click the **Add** button.
 - Step 3** Select the required server type.
 - Step 4** Complete the required fields and click the **Add** button.
-

The server is added to the system.

Procedure

Modifying an IVR Server

To modify an IVR Server:

- Step 1** Browse to *Network > IVR Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The server is updated with the changes.

Procedure

Deleting an IVR Server

To delete a server:

- Step 1** Browse to *Network > IVR Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the server is removed from the system.

Procedure

Testing the Server

To test a server:

- Step 1** Browse to *Network > IVR Servers*.
 - Step 2** Select the *Name* (active text link) of the server that you would like to test.
 - Step 3** Click the **Test** button.
-

The server is tested and the results displayed on screen.

SIP Application Servers

Procedure

Adding a SIP Application Server

To add a SIP Application Server to the Provider:

- Step 1** Browse to *Network > SIP Application Servers*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button next to the relevant available SIP Application server on the product list. The following SIP Application servers are available:
 - UC Central

Step 4 Provide the relevant server details. The following fields are available:

Field	Description	Remarks
Host Name	The host name of the SIP application server.	This is a mandatory field.
Description	An optional description for the server.	-
Software version	The SIP application server's software version.	This is a mandatory field.
IP Address	The IP address of the SIP application server.	This is a mandatory field.
Admin Username	The admin username for the SIP application server.	This is a mandatory field.
Admin Password	The Admin password for the SIP application server.	This is a mandatory field.
Monitor	Select the checkbox if you would like to monitor the SIP Application Server.	-
Out of Service	Select the checkbox if you would like to place the SIP Application Server out of service.	-
SIP Destination is a DNS SRV Record	Select the checkbox if the SIP Destination is a DNS SRV Record.	-
SIP Destination (CUPS Hostname or IP Address)	The SIP destination (CUPS Hostname or IP Address in the DNS.	This is a mandatory field.
CPID	The Call Processor ID for the SIP Application server. This is a mandatory field.	If you would like the system to automatically select the required value, select the Auto option, alternatively, select the required value from the drop-down list.
Manual mode	Select the checkbox if you would like the SIP Application server to be in manual mode.	Note For some SIP Application servers (e.g. UC Central), manual mode is always be pre-selected.
Email Address	Specify the email address for manual mode.	This is a mandatory field if the manual mode option has been selected.

Step 5 Click the **Add** button. On clicking the **Add** button, the following back-end transaction is triggered:

- AddInterwiseServer (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide)

Procedure

Modifying a SIP Application Server

To modify a SIP Application Server:

Step 1 Browse to *Network > SIP Application Servers*.

Step 2 Select the required SIP Application Server *name* (active text link).

Step 3 Modify the required fields. The following fields are available:

Field	Description	Remarks
Host Name	The host name of the SIP application server.	This is a mandatory field.
Description	An optional description for the server	-
Software version	The SIP application server's software version.	This is a mandatory field.
IP Address	The IP address of the SIP application server.	This is a mandatory field.
Admin Username	The admin username for the SIP application server.	This is a mandatory field.
Admin Password	The Admin password for the SIP application server.	This is a mandatory field.
Monitor	Select the checkbox if you would like to monitor the SIP Application Server.	-
Out of Service	Select the checkbox if you would like to place the SIP Application Server out of service.	-
SIP Destination is a DNS SRV Record	Select the checkbox if the SIP Destination is a DNS SRV Record.	-
SIP Destination (CUPS Hostname or IP Address)	The SIP destination (CUPS Hostname or IP Address) in the DNS.	This is a mandatory field.
CPID	The Call Processor ID for the SIP Application server.	The value cannot be modified.
Manual mode	Select the checkbox if you would like the SIP Application server to be in manual mode.	Note For some SIP Application servers (e.g. UC Central), manual mode is always be pre-selected.
Email Address	Specify the email address for manual mode.	This is a mandatory field if the manual mode option has been selected.

Step 4 Click the **Modify** button. On clicking the **Modify** button, the following back-end transaction is triggered:

- ModInterwiseServer (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide).

Procedure

Deleting a SIP Application Server

To delete a SIP application server:

Step 1 Browse to *Network > SIP Application Servers*.

- Step 2** Select the required *SIP Application Server* (active text link).
- Step 3** Click the **Delete** button. On clicking the **Delete** button, the following back-end transaction is triggered:
- DelInterwiseServer (in the case of an UC Central SIP Application server; for more information see the UC Central Provisioning Guide).

Note

- The first time that the SIP Application server is connected to the Unified CM, all the Subscribers in that CCM cluster is provisioned for the SIP Application server (provided the SIP Application server has been enabled in each subscriber server).
 - If a Subscriber is added at a later stage it has to be connected manually to the SIP Application server (see [Connecting or Disconnecting Subscribers to the SIP Application Server on page 142](#) if required).
-

[Connecting a CCM Cluster to a SIP Application Server on page 141](#)

Procedure

Disconnecting a CCM Cluster from a SIP Application Server

To disconnect a CCM cluster from a SIP application server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button next to the relevant CCM cluster on the list.
- Step 3** Click the **PBX=>Third Party Sip** button.
- Step 4** Click the **Disconnect** button associated with the relevant SIP Application server. On clicking the **Disconnect** button, the following back-end transaction is triggered:
- DisconnectInterwiseServer (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide).
-

Connecting a CCM Cluster to a SIP Application Server

Procedure

To connect a CCM cluster to a SIP application server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button next to the relevant CCM cluster on the list.
- Step 3** Click the **PBX=>Third Party Sip** button.
- Step 4** Click the **Connect** button associated with the relevant SIP Application server.
- Step 5** Complete the required fields. The following fields are available when connecting a CCM cluster to a SIP Application Server:

Field	Description	Remarks
Host Name	The name of the SIP Application server.	-

Field	Description	Remarks
Description	A short description of the SIP Application server.	
Software Version	The SIP application server's software version.	This is a mandatory field.
DN Prefix	A numeric value, used as a call routing prefix to identify the connection. Used as the start of the CTI Route Point DN created during the activation of the UC Central features for a user.	The maximum field length allowed is 20. Note Also available as a CCM model variable in various transactions.
DN Suffix	A numeric value, used as a call routing suffix to identify the connection. Used as the end of the CTI Route Point DN created during the activation of the UC Central features for a user.	The maximum field length allowed is 20. Note Also available as a CCM model variable in various transactions.
Connect UC Central SIP trunk templates	Select a SIP trunk template to use for the SIP trunk settings. The drop down list is populated by the templates defined in the CCM model.	Note This is matched against the template column in the CCM model for the SIP Trunks sheet in combination with the model name to determine which trunk definition to use.

Step 6 Click the **Connect** button. On clicking the **Connect** button, the following back-end transaction is triggered:

- ConnectInterwiseServer (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide).

Connecting or Disconnecting Subscribers to the SIP Application Server

Procedure

To connect or disconnect subscribers:

- Step 1** Browse to *Network > SIP Application Servers*.
- Step 2** Select the required *SIP Application Server* (active text link).
- Step 3** Click the **Advanced** button.
- Step 4** To connect a new Subscriber to the SIP Application server, click the **Connect** button associated with the relevant Subscriber in the *Available subscribers* section OR to disconnect a Subscriber from the SIP Application server, click the **Disconnect** button associated with the relevant Subscriber in the *Connected subscribers* section.

On clicking the **Connect** button, the following back-end transaction is triggered:

- ConCCMSubscriberInterwise (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide).

On clicking the **Disconnect** button, the following back-end transaction is triggered:

- DisconCCMSubscriberInterwise (in the case of a UC Central SIP Application server; for more information see the UC Central Provisioning Guide).

Note

If a subscriber is removed from the Unified CM cluster to which a SIP Application server is connected, the subscriber needs to be disconnected from the SIP Application server first.

Hardware Group Management

Hardware groups link the architecture components into groups. The transaction selects a device from the specified group that is available for the required purpose. For example, AddLocation selects an IPPBX and a transit switch from the devices in the specified hardware group. If multiple IPPBX are in the hardware group, the system selects one. The AddLocation transaction only configures one IPPBX selected from the hardware group (the system does not configure all IPPBXs in the hardware group).

Note

Hardware sets are used to determine if, for example, other IPPBXs require configuration when one IPPBX is configured.

Hardware Groups link the architecture components into groups. These groups allow the system to link specific hardware to a Location. This enables the system to manage tenants with multiple sites across multiple hardware groups.

Note

- You must be at the Service Provider Administrator level, or higher, to access this functionality.
 - Locations within a customer can use different hardware groups.
 - Hardware groups can contain multiple IPPBXs, the system automatically selects one based on least load.
 - Hardware groups cannot be modified in the system.
 - Devices can belong to more than one hardware group. There are no restrictions.
-

Hardware Groups are used at the customer and location levels:

- Customer

Hardware groups at the customer level are used to determine what devices to run the *AddCustomer* transactions against. The transaction runs against the IPPBX and Transit in the hardware group. The devices in the hardware group are stored with the customer as the *ippbxchosen* and transit chosen for future reference.

Note

If the *Enforcehcs* option is selected in the customer's active dial plan, the customer can manage what hardware groups are available to the locations. Only locations that are listed under the *Allowed Hardware Groups* section of the *Customer Hardware Group Management* page are accessible to the locations. A hardware group cannot be associated with more than one

customer. A device can be associated with more than one customer by including it in two different hardware groups. This is to support devices being shared between customers (e.g. aggregation, PBX if required, etc). Customer Administrators can access the *Customer Hardware Group Management* page by browsing to *General Administration > Customers > <Customer Name> > Advanced Mgt. > Hardware Group Association*.

- Location

There is no relation to the customer hardware group i.e. no default or inheritance. Hardware groups are required at the location level to define the devices which the *AddLocation* and other location level transactions run against. All location level transactions (e.g. FNN, phones, users, etc.) involve the device as defined in the location hardware group. For example, to add a conference service, you first add a hardware group that contains the required conference server. Then, when adding the conference service, you select the hardware group containing the appropriate conference server. If the location hardware group has more than one (1) IPPBX in it, the system automatically selects one based on the least load the system has for the cluster (number of lines allocated to the cluster).

The setup of the dial plan and architecture determines the required structure of your hardware groups. It is important that the *Transit* in the customer hardware group is included in the location's hardware group, otherwise, location dependencies on customer dial plans are broken. The location of IPPBXs in the location hardware groups is determined by how you would like to control hardware selection for the location. The IPPBX for the location can be different or the same as in the customer hardware group - there is no use of the *AddCustomer* model in the Cisco Unified Communications Manager model, so there are no dependencies on customer configuration at the location level. As noted above, you can have 2 locations in a customer with different hardware groups. To configure this, create your different hardware groups, then, when you add the location, select the hardware group you want to use (choose a different one for each location).

[Add a Hardware Group on page 144](#)

[View and Delete a Hardware Group on page 147](#)

Deleting a Hardware Group

Procedure

To delete a group:

- Step 1** Browse to *Network > Hardware Groups*.
 - Step 2** Select the *Name* (active text link) of the group that you would like to delete.
 - Step 3** Click the **Delete** button. After confirming the deletion, the group is removed from the system.
-

Note

Depending on the configuration of your system, confirmation may, or may not, be required when deleting a hardware group.

Add a Hardware Group

To add a hardware group:

Procedure

- Step 1** Browse to *Network > Hardware Groups*.

Step 2 Click the **Add** button on the *Hardware Group Management* screen. The *Add Hardware Group* screen is displayed.

Step 3 Complete all of the required fields, clicking the **Next** button when required to move to the next screen. The following fields are available when adding a Hardware Group:

Note

Depending on the configuration of your system, some of these fields may not be available.

Field	Description
Hardware Group Details	
Name	The name of the hardware group. This name must be unique in the system. This is a mandatory field.
Description	A short description of the group.
Limit usage of this Hardware Group to:	<p>Use this drop-down list to limit where the hardware group may be used. Options that may be selected include: <i>Any Action</i>, <i>Adding Console resources</i>, <i>Adding Contact Center resources</i>, <i>Adding Customers</i>, <i>Adding FNNs</i>, <i>Adding Locations</i>, <i>Adding Locations - Unmanaged Transit</i>, <i>Adding Locations - Unmanaged Legacy</i>, <i>Adding Voicemail resources</i>.</p> <p>Note</p> <p>The <i>Any Action</i> option refers to any action <i>other</i> than the available options. In order to make the hardware group available for a specific option, select the option from the list. Unmanaged PBX's will only be available to select and use in the Hardware Group if either the <i>Adding Locations - Unmanaged Transit</i> or <i>Adding Locations - Unmanaged Legacy</i> option is selected.</p>
Location Gateways	
This section contains two options, <i>Location Local Gateways</i> and <i>Location SRST Gateways</i> .	
<p>Notes:</p> <ul style="list-style-type: none"> Regardless of what action is selected for the hardware group, the <i>Location Gateways</i> settings are only relevant to the AssociateFNN transaction work flow, that is when the <i>Adding FNNs</i> option is selected from the <i>Limit usage of this Hardware Group to:</i> drop-down list (see above field). Either option or both (as required) must be selected for the associating FNNs transaction to work. The gateway(s) must already be configured and activated at the location level, these settings only configure the model related aspects of the gateway. The relevant Location Gateway settings are derived from the number range hardware group and not the hardware group assigned to the location. If the location does not have a gateway activated, no gateways are configured until one is activated. Configuration is based on the IOS model. 	
Location Local Gateways	Select the checkbox adjacent to <i>Location Local Gateways</i> if associateFNN logic should be used to configure the location's local gateway. This is required if the local gateways are using the P23 protocol and the dial plan has translation occurring on the gateway. When this checkbox is selected, the <i>LocalGW</i> option must be selected from the <i>PSTN Template</i> drop-down list on the <i>PSTN to Extn Range Mapping</i> screen (see External Numbers Range Management on page 827 if required).

Field	Description
Location SRST Gateways	Select the checkbox adjacent to <i>Location SRST Gateways</i> if associateFNN logic should be used to configure the location's SRST gateway. This is required if the SRST gateway needs configuration that relate to FNNs when in fall back mode.
Available Devices Note <ul style="list-style-type: none"> The following section of the screen varies depending on how your system is configured and what devices have been added to your system. If a Hardware Group is going to be used for a Voicemail Service and you intend to make use of an Auto Attendant service, make sure that an IVR server (for the AA service) is added to the Hardware Group at the same time as the Voicemail Server (for the Voicemail service). 	
Available PSTN Gateway Servers	This section lists all available PSTN Gateway servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Emergency Responder servers	This section lists all available Emergency Responder servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Transit Switches	This section lists all available Transit Switches. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available PBX systems	This section lists all available PBX systems. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group. It is mandatory to select at least one PBX system.
Available PBX Gateways	This section lists all available PBX Gateways. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Operator Consoles	This section lists all available Operator Consoles. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Music Servers	This section lists all available Music Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Voicemail servers	This section lists all available voicemail servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available IVR Servers	This section lists all available IVR Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Conference Servers	This section lists all available Conference Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
Available Contact Center Servers	This section lists all available Contact Center Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.

Step 4 Click the **Add** button when complete. The Hardware Group is added to the system.

View and Delete a Hardware Group

Note

Hardware groups can be viewed and deleted in/from the system, but not modified.

Procedure

Viewing a Hardware Group

To view a hardware group:

- Step 1** Browse to *Network > Hardware Groups*.
- Step 2** Select the *Name* (active text link) of the Hardware Group that you would like to view. Details of the selected Hardware Group are displayed.

The following fields are displayed when viewing a Hardware Group:

Note

Depending on the configuration of your system, some of these fields may not be available.

Field	Description
Hardware Group Details	
Name	The name of the hardware group. This is a read-only field.
Description	A short description of the group. This is a read-only field.
Limit usage of this Hardware Group to:	Displays where the hardware group may be used as selected when adding the hardware group (see Add a Hardware Group on page 144 for details if required). This is a read-only field.
Location Gateways	
This section contains two options, <i>Location Local Gateways</i> and <i>Location SRST Gateways</i> .	
Notes:	
<ul style="list-style-type: none"> Regardless of what action is selected for the hardware group, the <i>Location Gateways</i> settings are only relevant to the AssociateFNN transaction work flow. The gateway(s) must already be configured and activated at the location level, these settings only configure the model related aspects of the gateway. The relevant Location Gateway settings are derived from the number range hardware group and not the hardware group assigned to the location. If the location does not have a gateway activated, no gateways are configured until one is activated. Configuration is based on the IOS model. 	
Location Local Gateways	Select the checkbox adjacent to <i>Location Local Gateways</i> if associateFNN logic should be used to configure the location's local gateway. This is required if the local gateways are using the P23 protocol and the dial plan has translation occurring on the gateway.

Field	Description
Location SRST Gateways	Select the checkbox adjacent to <i>Location SRST Gateways</i> if associateFNN logic should be used to configure the location's SRST gateway. This is required if the SRST gateway needs configuration that relate to FNNs when in fall back mode.
Available Devices Note The following section of the screen varies depending on how your system is configured and what devices have been added to your system.	
<i>Available PSTN Gateway Servers</i>	This section lists all available PSTN Gateway servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Emergency Responder servers</i>	This section lists all available Emergency Responder servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Transit Switches</i>	This section lists all available Transit Switches. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available PBX systems</i>	This section lists all available PBX systems. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group. It is mandatory to select at least one PBX system.
<i>Available PBX Gateways</i>	This section lists all available PBX Gateways. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Operator Consoles</i>	This section lists all available Operator Consoles. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Music Servers</i>	This section lists all available Music Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Voice Mail servers</i>	This section lists all available voicemail servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available IVR Servers</i>	This section lists all available IVR Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Conference Servers</i>	This section lists all available Conference Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.
<i>Available Contact Center Servers</i>	This section lists all available Contact Center Servers. Select the checkbox(es) adjacent to the devices that you would like to include in the hardware group.

Procedure

Deleting a Hardware Group

To delete a hardware group:

- Step 1** Browse to *Network > Hardware Groups*.
- Step 2** Select the *Name* (active text link) of the Hardware Group that you would like to delete.

- Step 3** Click the **Delete** button. After confirming the delete operation, the Hardware Group is deleted from the system.

Note

Depending on the configuration of your system, confirmation may, or may not, be required when deleting a hardware group.

CCM Media Resource Group Management

Media resources include media resource groups and media resource group lists. Media resource management enables all CCMs in a cluster to share media resources including conferencing, transcoding, media termination, annunciator, and MOH services. Media resource groups and media resource group lists are added per CCM cluster.

Add a Media Resource Group

Media resources include media resource groups and media resource group lists. Media resource management enables all CCMs in a cluster to share media resources including conferencing, transcoding, media termination, annunciator, and MOH services. Media resource groups and media resource group lists are added per CCM cluster.

Procedure

To add a media resource group to a cluster:

- Step 1** Browse to the relevant cluster. The preferred path is from: *Network > PBX devices*
- Step 2** Select the **Name** (active text link) of the CCM cluster to which you would like to add the media resource group
- Step 3** Select the **Media Services** button
- Step 4** Select the **Media Resource Groups** button
- Step 5** Complete all of the required fields and select the **Add** button
-

The media resource group will be added to the system.

The following fields are available when adding a new media group:

Note: Depending on the configuration of your system, available fields may vary.

Details	
Field	Description
<i>Name</i>	The name of the media group. This is a mandatory field.
<i>Description</i>	A short description of the media group, optional.
<i>Multicast</i>	Select this checkbox if you would like the media group to have multicast functionality.

Select Servers
<p>Servers</p> <p>To add servers to the media resource group, select the servers from the <i>Available</i> list box and click Add >> to move them to the <i>Selected</i> list box.</p> <p>To modify the servers that have been added, select the servers from the <i>Selected</i> list box and click the << Remove button.</p> <p>To select all the servers in the <i>Available</i> or <i>Selected</i> list boxes, use the <i>Select All</i> link.</p> <p>When the required servers are listed in the <i>Selected</i> list box, click the Add button to add them to the media resource group.</p>

Note: When adding servers to the media resource group, only servers already associated with the cluster are displayed.

Modifying a Media Resource Group

Procedure

To modify a media resource group:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the media resource group that you would like to modify.
- Step 3** Click the **Media Services** button.
- Step 4** Click the **Media Resource Groups** button.
- Step 5** Select the *Name* (active text link) of the *Media Resource Group* that you would like to modify.
- Step 6** Modify the required fields and click the **Modify** button when complete. Refer to [Add a Media Resource Group on page 149](#) for field descriptions if required.

The media resource group is modified within the system.

Procedure

Deleting a Media Resource Group

To delete a media resource group:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the media resource group that you would like to delete.
- Step 3** Click the **Media Services** button.
- Step 4** Click the **Media Resource Groups** button.
- Step 5** Select the *Name* (active text link) of the *Media Resource Group* that you would like to delete.
- Step 6** Click the **Delete** button.

The media resource group is deleted from the system.

Adding a Media Resource Group List

Procedure

To add a media resource group List to a cluster:

- Step 1** Browse to *Network > PBX devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster to which you would like to add the media resource group list.
- Step 3** Click the **Media Services** button.
- Step 4** Click the **Media Resource Group Lists** button.
- Step 5** Click the **Add** button.
- Step 6** Complete all of the required fields. The following fields are available when adding a new media group list:

Field	Description	
Name	The name of the media group.	This is a mandatory field.
Description	A short description of the media group.	This is an optional field.
Media Resource Groups	Select the Media Resource Group Names, from the drop-down lists, that you would like to add to the media resource group list.	Only one Media Resource Group may be selected from each drop-down list, Media Resource Groups are added to the media group list in the order selected from the drop-down lists. There is no limit to the number of Media Resource Groups that can be selected. Each Media Resource Groups may only be added to the media group list once, for example, a Media Resource Groups may only appear in one drop-down list when adding a media group list.

- Step 7** Click the **Add** button. The media resource group list is added to the system.

Note

When adding media resource groups to a media resource group list, only media resource groups already associated with the cluster are displayed.

View and Modify Resource Lists

Media resources include media resource groups and media resource group lists. Media resource management enables all CCMs in a cluster to share media resources including conferencing, transcoding, media termination, annunciator, and MOH services. Media resource groups and media resource group lists are added per CCM cluster.

Procedure

Modifying a Media Group List

To modify a media resource group list:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the media resource group list that you would like to modify.
- Step 3** Click the **Media Services** button.
- Step 4** Click the **Media Resource Group Lists** button.
- Step 5** Select the *Name* (active text link) of the *Media Resource Group Lists* that you would like to modify.
- Step 6** Modify the required fields and click the **Modify** button.

The media resource group list is modified within the system.

The following fields are available when adding a new media group list:

Note

Depending on the configuration of your system, available fields may vary.

Field	Description
<i>Name</i>	The name of the media group. This is a mandatory field (on the Add screen only).
<i>Description</i>	A short description of the media group, optional.
<i>Media Resource Groups</i>	Select the Media Resource Group Names, from the drop-down lists, that you would like to add to the media resource group list. Only one Media Resource Group may be selected from each drop-down list, Media Resource Groups will be added to the media group list in the order that they were selected from the drop-down lists. There is no limit to the number of Media Resource Groups that can be selected. Each Media Resource Groups may only be added to the media group list once, for example, a Media Resource Groups may only appear in one drop-down list when adding a media group list.

Note

When adding Media Resource Groups to the media resource group lists, only Media Resource Groups already associated with the cluster are displayed.

Procedure

Deleting a Media Group List

To delete a media resource group list:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster that has the media resource group lists that you would like to delete.
- Step 3** Click the **Media Services** button.
- Step 4** Click the **Media Resource Group Lists** button.
- Step 5** Select the *Name* (active text link) of the *Media Resource Group Lists* that you would like to delete.
- Step 6** Click the **Delete** button.

The media resource group list is deleted from the system.

Associate a Media Resource Group List to a CCM

Procedure

To associate a list to a CCM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *CCM Name* (active text link) that you would like to assign the list to.
- Step 3** Click the **Trunk Config** button.
- Step 4** Select the relevant *Trunk* (active text link).
- Step 5** Select the relevant Media Resource Group List from the drop-down list then click the **Modify** button. The list is associated to the selected trunk.

Adding a CCM Group

Procedure

To create a new group within a cluster:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the CCM cluster to which you would like to add a group.
- Step 3** Click the **Groups** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields. The following fields are available when adding a group:

Field	Description	Remarks
Group Name	The name of the group being added.	This is a mandatory field.
Description	A short description of the group	-
Maximum Streams supported	Specify the maximum number of streams supported by the group.	This is a mandatory field.
Use for Phones	Select this checkbox if this group is going to be used for phones.	-
Use For Trunks	Select this checkbox if this group is going to be used for Trunks.	-
Use For Voicemail	Select this checkbox if this group is going to be used for voicemail.	-
Select Servers	Select the checkbox(s) adjacent to the servers that you would like to appear in this group.	-
Server Order	Use the drop-down list to specify the hierarchy of the servers. For example, if you would like Server 1 to be before Server 2, you would select 1 from the drop-down list adjacent to Server 1 and you would select 2 from the drop-down list adjacent to Server 2.	Note The server order is only changed when it is updated to a new server order number. Re-ordering does not happen automatically.

- Step 6** Click the **Submit** button. The group is added to the system.
-

Loading a PGW

Procedure

To load a PGW:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the PGW *Name* (active text link) that you would like to load.
- Step 3** Click the **Load** button. The PGW is loaded.
-

Loading a Cisco Unified Communications Manager (Unified CM) Cluster(s)

Procedure

To load a CCM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the CCM *Name* (active text link) that you would like to load.
- Step 3** Click the **Load static config** button. The CCM is loaded.
-

Provider Configuration

At this stage, all required PGWs and CCM clusters should be added and configured for your system. You are now required to configure aspects such as countries, customers and resellers. For more information on provider administration, please see Provider Administration section. The majority of this functionality can be added using the bulk loaders, for information on using bulk loaders (see [Bulk and Model Loader Functionality on page 543](#) for more information if required).

Legacy PBX Configuration and Management

Legacy PBX Configuration and Management includes IOS devices, unmanaged PBX devices, PSTN and E164 numbers as well as emergency published numbers.

Adding an IOS Device

For more information on IOS devices, see [IOS Device Management on page 205](#).

Procedure

To add an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button.

Step 3 Select the type of server that you would like to add and click the **Add** button.

Step 4 Complete the required fields. Available fields include:

Field	Remarks	Remarks
Device Details:		
Host Name	The host name of the IOS device.	This is a mandatory field.
Description	A short description of the IOS device you are adding.	-
Country	The country specific details to be applied to the device.	This is a mandatory field. Select the required country from the drop-down list.
Owner	Select the required owner from the drop-down list.	This is a mandatory field.
Single Location Only	This is mainly applicable to gateway device roles. When this setting is activated, the gateway type is set as local instead of central.	Select this checkbox if the device is only going to be utilized within one location.
Select Location	If you have selected the <i>Single Location Only</i> checkbox, you need to specify the location name here.	Select the required location from the drop-down list. Only one location can be selected.
Connectivity Details:		
IP Address	The IP address for the IOS device.	This is a mandatory field. This must be a unique IP Address within the provider.
IP Address (alternate)	An alternate IP address for the IOS device.	This must be a unique IP Address within the provider.
IP Domain	The domain within which the IP falls.	-
Cisco User Id Required	Select this checkbox if you would like the IOS device to require a Cisco User ID when accessed.	-
Config User Name	The user name of the person who managing the IOS device.	-
Config Password	The password for the Config user as described above.	This is a mandatory field.
Enable Password	Select this checkbox if you would like the IOS device to request the Config User's password when the access the device.	This is a mandatory field. We recommend that this option is selected.
Software Version	The IOS version that the device is running.	-
Manual Configuration Mode	Select this checkbox if you would like the IOS device to be manually configurable.	<p>Commands sent to the IOS device are still logged and can be accessed via the normal set of <i>IOS Command</i> screens.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>

Field	Remarks	Remarks
Email address for Manual activation	The email address used during the manual activation of the IOS device.	-
Network Monitoring active	Select this checkbox if you want to activate Network Monitoring on the IOS device.	-
<i>Detailed trace file of configuration sessions</i>	Select this checkbox if you would like to maintain a detailed trace file of all IOS device configuration sessions	-
Encrypt configuration sessions	Select this checkbox if you want to encrypt configuration sessions with the IOS device.	Encrypting configuration sessions is recommended, however, depending on the setup of your network, a reduction in performance may be experienced.
Device Roles:		
Gateway	Select this checkbox if the IOS device is a gateway.	After the IOS device has been added, this section lists all available gateways. To add a gateway, click the Add button. To modify a gateway, select the gateway's <i>Name</i> (active text link).
Media Resources	Select this checkbox if the IOS device is a Media Resource.	After the IOS device has been added, this section lists all available Media Resources. To add a Media Resource, click the Add button. To modify a Media Resource, select the Media Resource's <i>Name</i> (active text link).

Step 5 Click the **Finish** button when complete. The new IOS device is added to the system.

Unmanaged PBX Devices

Adding an Unmanaged PBX Device(s)

Procedure

To add an Unmanaged PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the Unmanaged PBX server.
- Step 4** Complete all of the required fields. The following fields are available when adding an Unmanaged PBX:

Field	Description	Remarks
Host Name	Host name of the server.	This is a mandatory field. This must be unique in the system.

Field	Description	Remarks
Description	A short description of the server	-
Country	The country in which the server is situated.	This is a mandatory field.
Email Address	The email address of the server administrator.	This is a mandatory field.
IPPBX CPID	Select the required CPID from the drop-down list	-
IPPBX CID	Select the required CID from the drop-down list.	This is a mandatory field.

Step 5 Click the **Add** button. The unmanaged PBX is added to the system.

View and Modify an Unmanaged PBX

The following tools are accessible from the *View and Modify an Unmanaged PBX* screen:

Tool/Task	Accessed By	Description
<i>Modify</i>	Clicking the Modify button.	To modify a clusters configuration, make the required changes then click the Modify button.
<i>Load</i>	Clicking the Load button.	This option loads configuration variables for the PBX. Note There is no confirmation before the configuration is loaded.
<i>Delete</i>	Clicking the Delete button.	This option deletes the CCM Server Cluster from the system. Note Depending on the configuration of your system, confirmation is required when deleting an IOS device.
<i>Test</i>	Clicking the Test button.	This option tests the PBX, the results of the test are displayed.

Unmanaged PBXs are often used as a parent component for a location.

Procedure

Modifying an Unmanaged PBX

To modify an Unmanaged PBX:

- Step 1** Browse to *Network > PBX devices*
- Step 2** Select the *Name* (active text link) of the Unmanaged PBX device that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

Note

Depending on the configuration of your system, some of these fields may not be available.

The Unmanaged PBX is modified within the system.

The following fields are available when modifying an Unmanaged PBX:

Field	Description
Server Name	Server name of the server. This must be unique in the system. This is a mandatory field.
Description	A short description of the server
Country	The country in which the server is situated. This is a mandatory Field
Email Address	The email address of the server administrator. This is a mandatory field.
IPPBX CPID	Call Processing ID - This is assigned to hardware as required, for example: PBX, PGW, Voicemail, etc. Select the required IPPBX CPID from the drop-down list. To use an automatic CPID, select the <i>Auto</i> option.
IPPBX CID	Cluster ID - This is the ID assigned to each Unified CM PBX cluster in the system. Select the required IPPBX CID from the drop-down list, alternatively, select the <i>Auto</i> option.

Procedure***Deleting an Unmanaged PBX***

To delete an Unmanaged PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the Unmanaged PBX device that you would like to delete
- Step 3** Click the **Delete** button

After confirming the deletion operation, the unmanaged PBX is removed from the system.

Procedure***Loading and/or testing an Unmanaged PBX***

To load or test an unmanaged PBX server:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the Unmanaged PBX device that you would like to configure
- Step 3** To load the server, click the **Load** button

or

To test the server, click the **Test** button

The system performs the specified task on the PBX.

Unmanaged PBX Server Tools

Server Tools enable administrators to perform advanced operations on Unmanaged PBX Servers. For more information on the available tools, please consult the relevant Feature Guide.

Adding the Unmanaged PBX to a Hardware Group

Procedure

Before you can deploy the unmanaged PBX to a location, it needs to be added to a hardware group. To add a hardware group:

- Step 1** Browse to *Network > Hardware Groups*.
 - Step 2** Click the **Add** button.
 - Step 3** Complete the required fields, ensuring you select the *unmanaged PBX*, then click the **Add** button. The hardware group containing the unmanaged PBX is added to the system.
-

Adding an Unmanaged PBX Location(s)

Locations based on unmanaged PBXs are added in a similar fashion to normal locations; the only difference is that a hardware group containing an unmanaged PBX is selected when adding the location. For steps on how to add a location, please see the Location Administration section.

For more information on unmanaged locations, please see the Unmanaged Locations section of the Location Administration section.

Adding PSTN Published Numbers

Procedure

To add PSTN published numbers to a location:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the location *Name* (active text link) to which you would like to add the PSTN published numbers.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the PSTN Published Number button.
 - Step 5** Complete all of the required fields then click the **Add** button. The PSTN Published number is added to the location.
-

Creating and Managing E164 Numbers

For more information on managing E164 numbers, see under [E164 Numbers on page 570](#).

Adding Emergency Published Numbers

Procedure

To add an emergency published number to a location:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) where you want to add the emergency published number.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Emergency Number** button.
 - Step 5** Complete all of the required fields and click the **Submit** button. The emergency published number is added to the location.
-

Provisioning Cisco Voice Messaging Services

This section describes the provisioning of Cisco Unity servers.

Provisioning Cisco Unity Connection

Cisco Unity Connection clusters are deployed in a similar manner as to other voicemail servers.

When deploying a Cisco Unity Connection cluster, the following must be noted:

- Templates must be added manually to the Cisco Unity Connection server
- The server option will only be available if the server has been added to a hardware set via *Dial Plan Tools > Hardware Sets*
- The hardware set needs to be associated with the dial plans by disconnecting and connecting them again.

Cisco Unity Connection Server Specifics

Versions

The system currently only supports the use of Cisco Unity Connection Server 8.

Passwords

The user password for the Cisco Unity Connection server is the same as the user's system password.

Server Sync Tool

When attempting to synchronize a voicemail server and the system's database via the *Tools* pages, an error can occur regarding users not being on the CUC server. The tool updates existing users on the voicemail server with existing user information from the system's database. If the user does not exist on the voicemail server, an error will occur. The tool makes no attempt to add the user to the voicemail server in this case.

Server Versioning Options

When setting up the server in the system, the user has the option to set the version to *Any* or alternatively to specify the exact version to be use. Should *Any* be selected, on connection with the server, the interface will detect the version being used by the server and then use the appropriate

library version to perform the transaction. Should the user specify a specific version, this library version will be used regardless of the server version.

Cluster Fall-Over Logic

The CUC is a cluster of two servers in an active-active state. When the system is attempting to perform transactions with the cluster the fall over logic will follow the below order of events:

Each transaction will attempt to connect and transact with the primary server.

Should the timeout be exceeded or the retry count be exceeded, the connection will be dropped and it will attempt to connect to the secondary server to perform the transaction.

Should the same fail conditions occur on the secondary server, the transaction will fail, and display an error message containing details about how many servers were attempted in the fall-over.

Cluster Fall-Over Timeout Setting

The Cisco Unity Connection supports being run in an active/active manner, that is, two servers may be configured, an active server and an auxiliary one.

Note

The timeout is not configurable by administrators via the GUI. The timeout can be configured via a constants file. The default is 40 seconds.

The system will initially attempt to contact the primary server, however, after a specified time-out period has elapsed, the system will attempt to contact the secondary server. If the secondary server is available, the transaction will complete as normal, if not, the system will return an error.

User SMS Notification Device and Voicemail User Templates

Currently, all templates used for creating voicemail account users with, must be created by the server administrator. The system uses *BasicVoiceMail* as default template if no other template is specified as via *Setup Tools > Service Types*.

Cisco Unity Connection requires an SMPP Provider (SMS gateway) be specified when a notification device is created for a user. The current CUC solution obtains this information from the template specified for the user. If SMS Notification Device functionality is required for users, then the template specified for those users must contain an SMS Notification Device with an SMPP Provider (mandatory field) associated with it.

Integrated Messaging Support

CUC Integrated Messaging is configured by means of a "class of service" assigned to a "subscriber template" in CUC. If the COS is configured to enable the user to have Integrated messaging, and associated to a Subscriber Template used to create a CUC user account, then the newly created user has the option of Integrated Messaging.

In the system, this process is assisted by giving the administrator options of selecting a "Subscriber Template" and an email address, when creating voicemail for a user. The email address configured here, would be the one used when setting up the Integrated CUC mailbox in the user's mail client.

Provisioning Cisco Unity

Pre-system Setup on Cisco Unity

Procedure

Follow these steps before deploying the system on Cisco Unity:

- Step 1** Install SQL Enterprise Tools on the physical Unity (Windows 2003 Server), in order to manage security and accounts for SQL.
- Step 2** Use SQL Authentication for the SQL server (specified in Enterprise Tools), and not Windows Authentication.
- Step 3** Create a new user under *Security - Logins* , and give it access to the Master and UnityDb databases.
- Step 4** Under each database, select Users, and create the same user, previously created, and give it the following roles: db_owner, db_datareader, db_datawriter.
- Step 5** Restart SQL to get the changes reflected.
-

The system does not automate the management of subscriber templates in Unity (add/mod/del). However any subscriber templates required can be added to Unity via the Unity GUI then a corresponding service type can be added into the system (the name of the service type needs to match the service type name exactly). There is one preloaded voicemail service type in the system called *BasicVoiceMail*.

At a minimum you should probably create a Subscriber Template called *BasicVoiceMail* in case it gets used.

Note

If you rename a subscriber template in Unity, the new name can't be used by the system. This is a flaw in Unity where it does not update the database with the correct values, so the system cannot access the subscriber template by the new name via the Unity stored procedures. If you need to rename, you are better creating a new subscriber template with a new name copying the old template.

Voicemail Setup

Multi Tenant Voicemail Set to On (Voicemail Service at the Customer Level - Default)

Procedure

- Step 1** Determine the voicemail service types required for the system.
- In a Cisco Unity based voicemail environment, the voicemail service types map to subscriber templates. As noted above in the Pre-system section, add any service types required for the subscriber templates (names must match exactly).
- Step 2** Adding the Unity Cluster via the GUI. Note that this can also be done via the loaders.
- a** Browse to Network > Voicemail Servers.
 - b** Click the **Add** button, and then select *Unity*.
 - c** Complete the following fields:
 - *Name*. Must be unique to this provider. This is a mandatory field
 - *Software Version*. This is a mandatory field.
 - *Email address for Manual activation*. This is a mandatory field for manual configuration mode.

- *Country*. This is a mandatory field.
- *Config User Id*. This is an optional field for manual configuration mode.
- *Config Password*. Password for the above account. This is an optional field for manual configuration mode.
- *Unity database access user ID*. This is an optional field for manual configuration mode.
- *Unity database access password*. This is an optional field for manual configuration mode.
- *IP Address*. IP address of the server. This is a mandatory field.

d Click the **Add** button.

Step 3 Create a Hardware Group with the Unity Server. Note that this can also be done via the loaders.

a Browse to Network > Hardware Group.

b Click the **Add** button.

c Enter a name and user then select your CCM and the Unity Server you just created.

Step 4 Create a Customer Voicemail Service.

Browse to *Resources > Voicemail Services* then enter the relevant details for the voicemail service, choosing the hardware group created above. On the next screen, select the required voicemail server.

Step 5 Create a Voicemail pilot for the Customer Voicemail Service above.

- View the details of the voicemail service created and click the Pilot Number button. Then click the **Add** button to add a pilot. Fill in the relevant details for the pilot and submit.

Note

- If the **extension** you need is not available, from the voicemail service details page select the internal number mgmt to allow the required extension.
- If the **site code** you need is not available in the drop-down, check the Customer site code inventory under the resources menu.
- If the **time zone** list is empty - this is currently populated based on the time zones in use by locations in the customer. So you may need to add a location in order to get a time zone to appear in the drop-down.

Step 6 Determine the voicemail service types allowed for the service.

Browse to *Resources > Voicemail Service*, select the voicemail service then click the **Voicemail Template Mgt** button. Any service types added to the system with the category voicemail should be available here. Select the ones required to be available to users of this voicemail service.

Step 7 Associate the Voicemail Service/Pilot with a Location.

Browse to required Location, click the **Advanced Mgt button**, and then click the **Voicemail Management** button. Click the **Voicemail Profile Mgt** button, and then click the **Add** button to create a new association. Enter the *Voicemail Profile Name*, the *Description* and the *Box Mask* and click the **Submit** button when complete to create the association as well as update any registered phones/user profiles in the location with the voicemail profile.

Note

- This can take some time if it is for a large location requiring a lot of setup.

- The **Voicemail Mgmt** button will not appear if there is not a voicemail service created for the customer.

Step 8 Create a voicemail box for a user.

- a Browse to *Location Administration > End Users*. From this page select the *Add* Link in the voicemail column -OR- select the user then select the voicemail box and the personal voicemail box. Enter the details for the user, selecting the appropriate line and entering a pin number. For the service type drop-down, select the appropriate setting.

Note

- The service type is populated based on the service types allowed in the system and via the voicemail service. The **Voicemail Profile Mgmt** button on the voicemail service details screen allows service types to be available for the voicemail service.
 - Default as a service type will use the voicemail service type from the user's feature group.
- b In the system, a voicemail box needs to be created for a user. The user needs to have some lines available either via an extension mobility profile or associated devices.

Step 9 Adding Alternate Extensions for a user.

- a Browse to *Location Administration > End Users > Personal Voicemail > Alternate Extensions*. Click the **Add** button and enter the extension you would like to use. This extension has to be unique within the Unity voicemail system (a user with this extension cannot already have voicemail, or already be added as an alternate extension by someone else).
- b Users can add a total of nine Alternate Extensions.

Step 10 Self Enroll at next login.

- The *Self Enroll on next login* option enables administrators to specify whether a user will have to listen to all the options available for configuring their account (Personal Greeting, Password, etc.) on their next login. To enable this feature, browse to *Location Administration > End Users (select the required end user) > Voicemail > Personal Voicemail*, then select the *Enabled* option from the drop-down list adjacent to the *Self Enroll on next login* field. Selecting this option sets this setting to ON on the Cisco Unity Connection server. Other available options include: *Disabled*, which sets this setting to OFF on the Cisco Unity Connection server, and *Ignore*, which does not change the setting on the Cisco Unity Connection server.

Multi Tenant Voicemail Set to Off (Voicemail Service at the Provider level)**Note**

When the Multi Tenant Voicemail setting is set to False, the Pilot for the voicemail service will be: SLC + Extension. When the setting is set to True, the code will automatically add the Inter Site Prefix in front of the Pilot: ISP +SLC+Extension. The recommended setting for HCS deployments is to have the setting set to False, as it allows the Pilot to be created in the correct format.

Caveat: One of the limitations of having the Multi Tenant setting to False in an HCS deployment is the fact that the voicemail service is not customer specific. Therefore the Admin who sets up the services would need to pay special attention in using the correct hardware and naming convention so that customers use their own services.

Procedure

- Step 1** Determine the voicemail service types required for the system.
- In a Cisco Unity based voicemail environment, the voicemail service types map to subscriber templates. As noted above in the Pre-system section, add any service types required for the subscriber templates (names must match exactly).
- Step 2** Adding the Unity Cluster via the GUI. Note that this can also be done via the loaders.
- Browse to *Network > Voicemail Servers*.
 - Click the **Add** button and select **Unity**.
 - Enter the following details and click the **Add** button.
 - **Config User Id:** Local windows admin account e.g. unityinstall.
 - **Password:** Password for the above account.
 - **DB User:** The user created with DB access in the Pre-system section.
 - **Password:** Password for the above user.
 - **IP Address:** IP address of the server.
- Step 3** Connect the Voicemail Server to the required Device (PBX/Transit).
- Note**
- This connection can also be made from the Transit/PBX side via the connectivity buttons.
- Browse to *Network > Voicemail Server* then click the **Connectivity** button next to the correct server. Select the appropriate connection (PBX/Transit) then select the appropriate device instance.
- Step 4** Create a Customer Voicemail Service.
- Browse to *Resources > Voicemail Services*, then enter the relevant details for the voicemail service and select the appropriate voicemail server.
 - The site code here is a text box as no site codes exist at the customer level. The site code used here should not be used in any customers as this will cause a conflict.
- Step 5** Create a voicemail pilot for the Customer Voicemail Service above.
- View the details of the voicemail service created and click the **Pilot Number** button. Then click the **Add** button to add a pilot. Fill in the relevant details for the pilot, including selecting the call agent (this will be populated by the transits/PBXs connect to the voicemail server) and submit. This will be the pilot for that particular integration between the voicemail server and the call agent.
- Note**
- If the **extension** you need is not available, from the voicemail service details page select the internal number mgmt to allow the required extension.
 - If the **site code** you need is not available in the drop-down, check the Customer site code inventory under the resources menu.
 - If the **time zone** list is empty - this is currently populated based on the time zones in use by locations in the customer. So you may need to add a location in order to get a time zone to appear in the drop-down.
- Step 6** Determine the voicemail service types allowed for the service.

- Browse to *Resources > Voicemail Service*. Select the voicemail service and select the **Voicemail Profile Mgmt** button. Any service types added to the system with the category voicemail should be available here. Select the ones required to be available to users of this voicemail service.

Step 7 Associate the Voicemail Service/Pilot with a Location.

- Browse to *Location > Advanced Management > Voicemail Mgt*. Click the **Add** button to create a new association. Name the association then select the appropriate voicemail service and pilot. The **Add** button just associates the service with the location. The **Add** and **Enable** button will create the association as well as update any registered phones/user profiles in the location with the voicemail profile (can take some time if a large location with a lot setup).

Note

The **Voicemail Mgmt** button will not appear if there is not a voicemail service created for the customer.

Step 8 Create a voicemail box for a user.

- a** Browse to *Location Administration > End Users*. From this page select the *Add Link* in the voicemail column -OR- select the user then select the voicemail box and the personal voicemail box. Enter the details for the user, selecting the appropriate line and entering a pin number. For the service type drop-down, select the appropriate setting.

Note

- The service type is populated based on the service types allowed in the system and via the voicemail service. The voicemail profile mgmt button on the voicemail service details screen allows service types to be available for the voicemail service.
- Default as a service type will use the voicemail service type from the user's feature group.
- b** In the system a voicemail box needs to be created for a user. The user needs to have some lines available either via an extension mobility profile or associated phones.

Step 9 Adding Alternate Extensions for a user.

- a** Browse to *Location Administration > End Users > Personal Voicemail > Alternate Extensions*. Click the **Add** button, and enter an extension you would like to use. This extension has to be unique within the Unity voicemail system (a user with this extension cannot already have voicemail, or already be added as an alternate extension by someone else).
- b** Users can add a total of 9 Alternate Extensions.

Step 10 Self Enrollment at next logon.

- Browse to *Location Administration > End Users > Personal Voicemail*. Select the checkbox next to *Self Enrollment at next logon*, to enable a user to listen to all the options available for configuring their account (Personal Greeting, Password, etc), when they logon the next time.

Hardware Transactions (for MT mode False - Provider Level Voicemail Service)

1. AddVMService.

- a.** This transaction will call the CCM driver to make a model call looking for any elements outlined with the model name *AddVMService-Unity*. This model will be run against any Cisco Unified Communications Manager (Unified CM) PBXs connected to the voicemail server the service belongs to.

- b. This transaction will call the PGW driver to make a model call looking for any mml outlined with the mmlscriptname *AddVMService-Unity*. This model will be run against any PGWs connected to the voicemail server the service belongs to.
 - c. This transaction will also call the voicemail driver but there is currently nothing being applied to the Unity server.
2. AddVMServicePilot.
 - a. This transaction will call the CCM driver to make a model call looking for any elements outlined with the modelname AddVMServicePilot-Unity. This model will only be run against any Unified CM servers if they were the selected CallAgent for the pilot.
 - b. This transaction will call the PGW driver to make a model call looking for any mml outlined with the mmlscriptname *AddVMService-Unity*. This model will only be run against any PGWs if they were the selected CallAgent for the pilot.
 - c. This transaction will also call the voicemail driver but there is currently nothing being applied to the Unity server.
3. AddActivateLocationVM - OR- AddLocationVM.
 - a. This transaction will add a VMProfile and VMPilot to the Unified CM server supporting the location the Voicemail service is being associated with. The pilot will be the first of the pilot created for the service and the CSS will be the CSS mapped to the COS Service type *Voicemail*. The VMProfile will be called *vmprofile* and have the location-id added to the end of the name. These are created in the PBX for each location the voicemail service is associated with (so if a system-wide CSS is used, this could cause duplicate issues).
 - b. This transaction will call the CCM driver to make a model call looking for any elements outlined with the modelname AddLocationVM-Unity. This model will only be run against the Unified CM server supporting the location the voicemail service is being assigned to.
 - c. This transaction will call the PGWdriver to make a model call looking for any mml outlined with the mmlscriptname *AddVMService-Unity*. This model will only be run against any PGWs that were the selected CallAgent for the pilot.

Technical Notes

Note for Hardware Groups

If type is ANY then PBX is required. For voicemail, should setup with just voicemail, then no PBX is required.

- connectIPPBXVoicemail
- driver_ippbx

Calls partition, css, routepattern, transpattern, transformpattern models with following variables:

- #VMNAME# = voicemail server name
- #CPID# = CPID for the voicemail server
- #VMCPID# = CPID for the voicemail server
- #MWIRID# = value equal to the all 9's for the length of the rid
- #SITECODE# = value equal to all 9's for the max length of the site code;
- #MWIPARTITION# = \$global_mwi_partitionname;
- #GLBLTRKDP# = \$global_trunk_device_pool;

If MT voicemail = F, then calls AddVMService for each VMService currently in the system for that VM Server to update the new connected PBX with the AddVMService details.

- addvmservice
- Driver_IPPBX for MT = true
- modelname = AddVMService-\$networktype

Talk to the first CCM selected from the hardware group for the VM service (random = first) model calls. If there is no PBX in the hardware group, will do nothing. Calls partition, css, routepattern, transpattern, transformpattern models with the following variables:

- #LOCATIONNUM# = Location ID for the virtual VM location.
- #VMSLC# = Site Code for the VMService.
- #VMCPID# = CPID assigned to the VM Server.
- #VMRID# = the RID for the voicemail service.

Driver_IPPBX for MT = false.

AddPSTNPubNum

Same as *AddLocationPubNum* in the PBX driver.

AddVMServicePilot

Driver_IPPBX

modelname = AddVMServicePilot-\$networktype.

Talk to the first CCM selected from the hardware group for the VM service (random = first) model calls or the call agent if passed. If there is no PBX in the hardware group or call agent passed, then does nothing.

Calls partition, css, routepattern, transpattern, transformpattern models with following variables:

- #GLOBALSITEPARTITION# = partition name read from the global settings.
- #PILOT# = \$pilotnumber = pilot number fint assigned to the vmservice.
- #VMNAME# = hostname of the voicemail server used for the service.
- #ISP# = intersite prefix for the customer.
- #CUSTOMER# = id of the customer in the system.
- #LOCATIONNUM# = location id assigned to the voicemail virtual location.
- #VMSLC# = site code of the voicemail service.
- #VMCPID# = cpid of the voicemail server for the voicemail service.
- #VMRID# = rid assigned to the voicemail service.

AddLocationVM

Driver_IPPBX

modelname = LocationVM-\$networktype

CSS used for the voicemail pilot is the CSS mapped to the 'Voicemail' COS.

Calls partition, css, routepattern, transpattern, transformpattern models with following variables:

- #DIALABLEFINT# = diallable voicemail pilot number.
- #LOCATIONNUM# = the system's location ID for the location.
- #ISP# = Intersite prefix for the location.
- #VMSLC# = site code assigned to the voicemail service.
- #VMCPID# = CPID assigned to the voicemail server.
- #VMRID# = RID assigned to the voicemail service.

Voicemail Pilot in Cisco Unified Communications Manager (Unified CM)

If the pilot/css combo does not exist in Unified CM, then it creates the voicemail pilot in Unified CM. The pilot is equal to the diallable pilot and CSS is the CSS mapped to the Voicemail COS.

Profile in Cisco Unified Communications Manager

Checks to see if the profile name/pilot/css combo exists, if not, it adds it. Name logic is:

Voicemail Profile Name Logic

If MT voicemail = true

vmprofile name = VMprofile#vmprofilenumber#

If MT voicemail = false

vmprofile name = VMP-#diallablepilotnumber#

If css for voicemail is customer_specific, voicemail profile name will include customer id (-customerid if MT=false). If css for voicemail is location specific, voicemail profiles name will include location id (-locationid if MT = false).

AddActivateLocationVM

Same as above, except it calls a OpsBulkPhoneModify, OpsBulkModMobility after completing the above work to update the phones/mobility profiles with the voicemail profile created.

AddAAService

Internal transaction only - doesn't talk to hardware.

AddAAServicePilot

Driver_IPPBX

Modelname = AddAAServicePilot-\$networktype

Calls partition, css, routepattern, transpattern, transformpattern models with following variables:

- #GLOBALSITEPARTITION# - partition
- #PILOT# - pilot number
- #AANAME# - auto attendant service name
- #AACOMPANYNAME# - auto attendant company name
- #ISP# - intersite access prefix

- #CUSTOMER# - customer id
- #LOCATIONNUM# - location id
- #AASLC# - site code
- #AAPID# - cpid
- #AARID# - rid

Cisco Unity Connection Auto Attendant Support

The system supports provisioning of the Cisco Unity Connection Auto Attendant (AA) as follows:

- A Cisco Unity Connection server can assume the role of both voicemail server and Interactive Voice Response (IVR) server.
- Adding an AA Service Pilot number creates a route pattern on the Cisco Unified Communications Manager (Unified CM) server which points at the Cisco Unity Connection server.
- Associating an E164 number to the service level pilot number provisions the PGW with the E164 number and points it at the Unified CM server which is connected to the Cisco Unity Connection server.
- Associating the AA service to a location enables the location admin to associate an E164 number to the internal pilot number to be routed to the location via a LBO gateway.
- All Cisco Unity Connection Auto Attendant specific setup, e.g. Call Handlers, Schedules etc. is done via the Cisco Unity Connection GUI which is cross launched from the system.

Note

This feature is only available when **MultiTenantVoicemail** is set to 'ON' at the provider level.

Enable the IVR role on Cisco Unity Connection

A Cisco Unity Connection Voicemail Server can also assume the role of IVR server. A Cisco Unity Connection Voicemail Server will always keep its role as Voicemail Server even when the role of IVR Server is enabled.

When a Cisco Unity Connection Server has the IVR server role enabled, it will be available via *Network > IVR Servers* in addition to *Network > Voicemail Servers*

The IVR role can be enabled when a new voicemail or IVR server is added or by modifying an existing voicemail or IVR server.

Add a Voicemail Server with IVR server role

Procedure

To add a Voicemail server with the IVR server role:

- Step 1** Browse to *Network > Voicemail Servers*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button next to *UnityConnection*.
- Step 4** Complete the required information.

- Step 5** In the *Roles* section, select the *IVR server* checkbox.
- Step 6** Click the **Add** button.

Add an IVR Server

Procedure

To add an IVR server with the IVR server role:

- Step 1** Browse to *Network > IVR Servers*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button next to *UnityConnection*.
- Step 4** Complete the required information.
- Step 5** In the *Roles* section, the *IVR server* checkbox will be checked by default.
- Step 6** Click the **Add** button.

This will create a new Voicemail serve as well as a new IVR Server.

Enable/Disable IVR on an existing Voicemail Server

Procedure

To enable or disable IVR on a voicemail server:

- Step 1** Browse to *Network > Voicemail Server*.
- Step 2** Select the relevant Voicemail Server.
- Step 3** In the *Roles* section, select or deselect the *IVR* checkbox.
- Step 4** Click the **Modify** button.

Enable/Disable IVR on an existing IVR Server

To enable or disable IVR on an IVR server:

Procedure

- Step 1** Browse to *Network > IVR Servers*.
- Step 2** Select the relevant IVR Server.
- Step 3** In the *Roles* section, select or deselect the *IVR* checkbox.
- Step 4** Click the **Modify** button.

Note

The IVR Server will be removed from the IVR index page if the IVR role is removed from either the Voicemail Server screen or the IVR screen.

Auto Attendant Services

An Auto Attendant Service can be created and associated to a specific Voicemail Service at Customer Level.

Adding an AA Service Pilot number creates a route pattern on the Cisco Unified Communications Manager (Unified CM) server that points at the Cisco Unity Connection server.

Associating an E164 number to the service level pilot number provisions the PGW with the E164 number and points it at the Unified CM server that is connected to the Cisco Unity Connection server.

Add an Auto Attendant Service at Customer Level

Prerequisites:

To create an Auto Attendant Service the following needs to be in place:

- A Cisco Unity Connection Server with IVR enabled
- A hardware group that contains the above Cisco Unity Connection Server
- A Customer that is associated to the above Hardware Group
- A Voicemail Service with a configured pilot number

Add Voicemail Service

Procedure

To add a voicemail service:

- | | |
|---------------|--|
| Step 1 | Browse to <i>Resources > Voicemail Services</i> . |
| Step 2 | Click the Add button. |
| Step 3 | Complete the required information. |
| Step 4 | Click the Next button. |
| Step 5 | Complete the required information. |
| Step 6 | Click the Next button. |
| Step 7 | Click the Add button. |
-

Add Voicemail Pilot Number

Procedure

To add a voicemail pilot number:

- | | |
|---------------|--|
| Step 1 | Browse to <i>Resources > Voicemail Services</i> . |
| Step 2 | Select the relevant Voicemail Service. |
| Step 3 | Click the Pilot Number button. |
| Step 4 | Click the Add button. |
| Step 5 | Complete the required information. |

- Step 6** Click the **Add** button.
-

Add Auto Attendant Service

Procedure

To add an Auto Attendant service:

- Step 1** Browse to *Resources > Auto Attendant Services*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required information.
- Step 4** Click the **Next** button.
- Step 5** Select an appropriate IVR Server from the drop-down list.
- Step 6** Click the **Next** button.
- Step 7** Select a Voicemail Service from the drop-down list.
- Step 8** Click the **Add** button.
-

Auto Attendant Pilot Number Management

A pilot number is the address or location of a group, or feature, within a PBX or IP-PBX and is generally defined as a blank extension number or an extension that does not have a person or telephone associated with it. When using an auto attendant service, each service must be associated to a pilot number. The pilot number is used to locate the service and in turn to locate the telephone extension number on which the incoming call was received. Without a defined pilot number, the PBX or IP-PBX cannot locate where the incoming call was received.

Note

Before assigning a pilot number, please ensure that there are available pilot numbers within your system.

Procedure

Add AA service level Pilot Numbers

To add a pilot number for an auto attendant service:

- Step 1** Browse to *Resources > Auto Attendant Services*.
- Step 2** Select the relevant Auto Attendant Service.
- Step 3** Click the **Pilot Numbers** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required information.
- Step 6** Click the **Next** button.
- Step 7** Complete the required information.
- Step 8** Click the **Add** button.
-

Procedure

Deleting a Pilot Number

To delete a pilot number:

- Step 1** Browse to *Resources > Auto Attendant Services*
 - Step 2** Select the Auto Attendant (Active text link) that you would like to delete a pilot number from.
 - Step 3** Select the Pilot Number button
 - Step 4** Select the Pilot Number (Active text link) that you would like to delete
 - Step 5** Select the **Delete** button
-

After confirming the deletion operation, the pilot number will be deleted from the service.

Associate an E164 number to the AA Service level pilot

Prerequisites:**Procedure**

To be able to associate an E164 number to the AA service level pilot number, a range of E164 numbers has to be moved to the VM Service that is associated with the AA service at Customer level; follow these steps:

- Step 1** Browse to *Resources > E164 Inventory*.
 - Step 2** Select the appropriate Country from the drop-down list.
 - Step 3** Click the **Next** button.
 - Step 4** Select the appropriate National Area Code from the drop-down list.
 - Step 5** Click the **Next** button.
 - Step 6** Click the **Move Number Range** button.
 - Step 7** Select the appropriate Number Range and Location.
 - Step 8** Click the **Move** button.
-

Associate an E164 number to the AA Service level pilot

Procedure

To associate an E164 number to the AA Service level pilot number:

- Step 1** Browse to *Resources > Auto Attendant Services* .
- Step 2** Select the relevant AA Service.
- Step 3** Click the **PSTN Number Mgt** button.
- Step 4** Click the **Associate Range** button.
- Step 5** Complete the required fields.
- Step 6** Click the **Submit** button.

Location Auto Attendant Services

Associating the AA service to a location enables the location admin to associate an E164 number to the internal pilot to be routed to the location via a LBO gateway.

Add a Location Auto Attendant Service

Procedure

To add an auto attendant service at location level:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the relevant Location.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Auto Attendant** button.
 - Step 5** Click the **Add** button.
 - Step 6** Complete the relevant information.
 - Step 7** Click the **Add** button.
-

Associate an E164 number to the internal pilot

Prerequisites:

Procedure

To be able to associate an E164 number to the Location AA pilot a range of E164 numbers has to be moved to the Hardware Group and Location; follow these steps:

- Step 1** Browse to *Resources > E164 Inventory*.
 - Step 2** Select the appropriate Country from the drop-down list.
 - Step 3** Click the **Next** button.
 - Step 4** Select the appropriate National Area Code from the drop-down list.
 - Step 5** Click the **Next** button.
 - Step 6** Click the **Move Number Range** button.
 - Step 7** Select the appropriate Number Range and Location.
 - Step 8** (It needs to be the appropriate Hardware Group at Location Level.)
 - Step 9** Click the **Move** button.
-

Associate an E164 number to the internal pilot

Procedure

To associate an E164 number to an internal pilot number:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the relevant Location.
 - Step 3** Click the **Advanced Management** button.
 - Step 4** Click the **Auto Attendant** button.
 - Step 5** Select the appropriate Location AA Service.
 - Step 6** Click the **Associate Range** button.
 - Step 7** Select the appropriate National Code
 - Step 8** Click the **Next** button.
 - Step 9** Specify a number range.
 - Step 10** Click the **Next** button.
 - Step 11** Select the appropriate range.
 - Step 12** Click the **Submit** button.
-

Cisco Unity Connection AA Specific Functionality Setup

All Cisco Unity Connection Auto Attendant specific setup, e.g. Call Handlers, Schedules, etc. are set up via the Cisco Unity Connection Admin GUI, which is cross launched from the system.

Cross launch the Cisco Unity Connection Admin GUI from the system

Procedure

- Step 1** Browse to *Resources > Auto Attendant Services*.
 - Step 2** Select the relevant AA Service.
 - Step 3** Click the **Configure IVR** button.
 - Step 4** Depending on the browser settings, the Cisco Unity Connection Admin GUI login screen is opened in a separate window or tab.
-

Provisioning the Local PSTN Breakout Support

Procedure

To provision Local PSTN Breakout Support:

- Step 1** Add an IOS Device by following these steps:
 - a** Browse to *Network > IOS Devices*.
 - b** Click the **Add** button.
 - c** Click the **Custom Add** button.
 - d** Complete the required fields. Ensure that the *Single Location Only* field is selected (if applicable).
 - e** In the section *Device Roles*, select the *Gateway* checkbox.

- f Click the **Add** button.

For more information on adding an IOS Device, see [IOS Device Management on page 205](#).

Step 2 Add a Gateway by following these steps:

- a Browse to Network > IOS Devices.
- b Click on the relevant IOS Device host *Name* (active text link).
- c In the Device Roles section, click the **Add** button.
- d Provide the required information. Ensure that the correct Protocol is selected from the drop-down list (e.g. SCCP, MGCP, H.225 or SIP).
- e Click the **Next** button.
- f On the next screen, select the device from the *Select Device* drop-down list and click the **Next** button.
- g On the next screen, in the *Gateway Functions* section, select *PSTN Local*. Note that *Analog* is optional and can be run in combination with the PSTN role.
- h Click the **Add** button.

Step 3 Configure the Gateway and Interfaces by following these steps:

- a Browse to *Network > IOS Devices*.
- b Click on the relevant IOS Device host *Name* (active text link).
- c In the *Device Roles (Gateway Details)* section, click on the *Name* (active text link) of the relevant gateway.
- d In the Interface Details section, click the **Gateway Hardware Configuration** button.
- e Complete the required fields.
- f Click the **Modify** button.
- g Return (browse) to the gateway's *Interface Details* section and click the **Gateway Hardware Configuration** button.
- h Click the **Add Port** button.
- i On the next screen, select a *Port Type* from the drop-down list. (Only the E1, T1 and BRI options are applicable to the PSTN role.). Provide the port number and optionally the port range.
- j Click the **Add** button.
- k Return (browse) to the gateway's Interface Details section and click the **Gateway Hardware Configuration** button.
- l In the *Ports* section, the ports that have been added are displayed, but in an un-configured state. Select the relevant port(s) and click the **Configure Selected** button.
- m The port configuration details can be updated or left as provided (default values).
- n Click the **Next** button.
- o On the next screen, update gateway port configuration details, if required.
- p Click the **Add** button. The port will now be configured.

Step 4 Activate the Local Gateway Dial Plan by following these steps:

- a** For the relevant location, browse to *Location Administration > Telephony*.
- b** Click *Gateways* (active text link).
- c** Select the gateway's port/s that you wish to enable for the call routing.
- d** Click the **Activate** button.
- e** Select the relevant *Class of Service* from the drop-down list.
- f** In the *Call Agent Order* section, arrange the ports according to priority, if more than one is being added.
- g** Click the **Add** button.

Netwise

Add a Netwise Cluster

Procedure

To add a Netwise Cluster:

- Step 1** Browse to the relevant sub-menu under the *Network* menu.
- Step 2** Click the **Add** button.
- Step 3** If asked to specify what type of server you would like to add, click the **Add** button adjacent to the server type that you would like to add. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and click the **Add** button.

The Netwise Cluster is added to the system.

The following fields are available when adding a Netwise Cluster:

Note: Depending on the configuration of your system, some of these fields may not be available

Field	Description
Name>	Name for the Netwise server. Must be unique in the system. This is a mandatory field.
Description	A short description of the server.
Software Version	Select the software version that the server will be running, alternatively, you can select the Any option. This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that will be used for manual activation of the Server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
Country	Country where the Netwise server will be situated. This is a mandatory field.

Field	Description
Config User ID	The user name for configuring the server. This is a mandatory field.
Config Password	The password to be used when configuring the server. This is a mandatory field.
CMG database access user ID	The CMG database access user ID. This is a mandatory field.
CMG database access password	The CMG database access password. This is a mandatory field.
Detailed trace file of configuration sessions ?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.
Host Name	Host name for the server. Must be unique in the system. This is a mandatory field.
WINS	The Windows Internet Name Service (WINS) hostname that will resolve to the server's IP address. This is a mandatory field.
IP Address	IP Address for the server. This is a mandatory field.
Host offers ANA Authentication service	Select this checkbox if the server offers ANA Authentication service.
Host offers CWI interface to CMG database	Select this checkbox if the server offers CWI interface to CMG database.
Host offers TCS interface to Call Manager(s)	Select this checkbox if the server offers TCS interface to Unified CMs.
Host provides Line State Server facility	Select this checkbox if the server provides Line State Server facility.

View and Modify a Netwise Cluster

To modify a Netwise Cluster:

Procedure

- Step 1** Browse to the relevant sub-menu under the *Network* menu.
- Step 2** Select the **Name** (active text link) of the Netwise Cluster that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.

The Netwise Cluster is modified within the system.

The following fields are available when modifying a Netwise Cluster:

Note: Depending on the configuration of your system, some of these fields may not be available

Field	Description
Name	Name for the Netwise server. Must be unique in the system. This is a mandatory field.
Description	A short description of the server.

Field	Description
Software Version	Select the software version that the server will be running, alternatively, you can select the Any option. This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that will be used for manual activation of the Server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
Country	Country where the Netwise server will be situated. This is a mandatory field.
Config User ID	The user name for configuring the server. This is a mandatory field.
Config Password	The password to be used when configuring the server. This is a mandatory field.
CMG database access user ID	The CMG database access user ID. This is a mandatory field.
CMG database access password	The CMG database access password. This is a mandatory field.
Detailed trace file of configuration sessions ?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.
Host Name	Host name for the server. Must be unique in the system. This is a mandatory field.
WINS	The Windows Internet Name Service (WINS) hostname that will resolve to the server's IP address. This is a mandatory field.
IP Address	IP Address for the server. This is a mandatory field.
Host offers AnA Authentication service	Select this checkbox if the server offers AnA Authentication service
Host offers CWI interface to CMG database	Select this checkbox if the server offers CWI interface to CMG database
Host offers TCS interface to Call Manager(s)	Select this checkbox if the server offers TCS interface to Unified CMs
Host provides Line State Server facility	Select this checkbox if the server provides Line State Server facility

SIP Normalization Scripts Management

SIP Transparency and Normalization is implemented as a Lua script on the Unified CM. The script is associated to a SIP trunk to provide SIP protocol transparency and normalization of messages. Parameters can also be added for the script when associating the script to a SIP trunk.

This functionality is only provided on Unified CMs with version 8.5 +.

Procedure

Viewing SIP Normalization Scripts

To view SIP Normalization Scripts:

- Step 1** Browse to *Network > PBX Devices* .
- Step 2** Select the relevant PBX.

Note

SIP Normalization Scripts can only be imported/added for a PBX of Cisco Unified Communications Manager version 8.5 or later.

- Step 3** Click the **Import/Refresh Items** button.
 - Step 4** Select *SIP Normalization Scripts* (active text link). On the next screen the scripts that have been added or imported for the PBX are displayed.
-

Procedure

Importing SIP Normalization Scripts

To import SIP Normalization Scripts:

- Step 1** Browse to *Network > PBX Devices* .
- Step 2** Select the relevant PBX.

Note

SIP Normalization Scripts can only be imported/added for a PBX of Cisco Unified Communications Manager version 8.5 or later.

- Step 3** Click the **Import/Refresh Items** button.
 - Step 4** Select the checkbox adjacent to *SIP Normalization Scripts*.
 - Step 5** Click the **Import/Refresh Items** button.
-

Procedure

Adding SIP Normalization Scripts

To add SIP Normalization Scripts:

- Step 1** Browse to *Network > PBX Devices* .
- Step 2** Select the relevant PBX.

Note

SIP Normalization Scripts can only be imported/added for a PBX of Cisco Unified Communications Manager version 8.5 or later.

- Step 3** Click the **SIP Normalization Scripts** button.
- Step 4** Click the **Add New Script** button. The following fields are available:

Field	Description	Remarks
Script Name	The name of the Normalization Script.	-
Description	A short description of the script.	-
Content	The actual content of the script.	-
Script Execution Error Recovery Action	Indicate the action that should be taken when an execution error is encountered while the script is being run.	Select from the drop-down list one of the following options: <i>Message Rollback Only</i> , <i>Disable Script</i> , <i>Reset Script</i> , <i>Reset Trunk</i> .
System Resource Error Recovery Action	Indicate the action that should be taken when a resource error is encountered while the script is being run.	Select from the drop-down list one of the following options: <i>Disable Script</i> , <i>Reset Script</i> , <i>Reset Trunk</i> .
Memory Threshold	The memory limit of the script.	Default value: 50 kilobytes.
Lua Instruction Threshold	The content limit of the script.	Default value: 1000 Lua code instructions.

Step 5 Click the **Add** button.

Procedure

Adding a Shared Script

To add a Shared SIP Normalization Script:

Step 1 Browse to *Network > PBX Devices* .

Step 2 Select the relevant PBX.

Note

SIP Normalization Scripts can only be imported/added for a PBX of Cisco Unified Communications Manager version 8.5 or later.

Step 3 Click the **SIP Normalization Scripts** button.

Step 4 Click the **Add Shared Script** button.

Step 5 Select *SIP Normalization Script* from the drop-down list. The available options (scripts) are all the Normalization Scripts that have been added to the system already, for all PBXs of the same Provider as the current PBX.

Step 6 Click the **Next** button. On the next screen all the details of the shared script are displayed.

Procedure

Modifying a SIP Normalization Script

To modify a SIP Normalization Script:

Step 1 Browse to *Network > PBX Devices* .

Step 2 Select the relevant PBX.

Step 3 Click the **SIP Normalization Scripts** button.

- Step 4** Select the Script *Name* (active text link). On the next screen all the details of the shared script are displayed.
- Step 5** Update the details of the script and click the **Modify** button.

Associating the SIP Normalization Script to a Connection

To associate the SIP Normalization Script to a SIP trunk used by a connection between PBX'S:

Procedure

- Step 1** Browse to *Network > PBX Devices* .
- Step 2** Click the **Connectivity** button of the relevant PBX.
- Step 3** Click the **PBX ==> PBX** button.
- Step 4** In the Managed PBX's section (PBX Clusters Not Connected To), select the PBX to connect to, and then click the **Connect IPPBX** button.
- Step 5** Provide the necessary connectivity details. The following fields are available:

Field	Description	Remark
Trunk Protocol	Select the relevant protocol from the drop-down list.	-
Topology Type	The options include "Star" and "Full Mesh". Star option will result in connectivity between the selected source cluster and the rest of the selected clusters. There will be no connection between the secondary / target clusters. Full Mesh option will connect all clusters participating in the selection between each other as well as the originating cluster.	Select from the drop-down list. Default option = Full Mesh.
Trunk Name	The available trunks which will be used for the connection between the PBX's.	This is a display field only.
Description	A description of the trunks.	-
SIP Profile	Lists the available SIP Profiles to apply to the connection.	Select from the drop-down
Normalization Script	Lists the available Normalization Scripts to apply to the connection.	Select from the drop-down
Script Parameters	Key-value pairs to be used by the script.\	Supplied in the format of key=value;key2=value2;key3=value3

- Step 6** Click the **Confirm** button.

Modifying the Trunk Details of a Managed-to-Managed Connection

Procedure

- Step 1** Browse to *Network > PBX Devices*.

- Step 2** Click the **Connectivity** button adjacent to the relevant cluster.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** In the PBX Clusters Currently Connected to <PBX Name> section, click the **Trunk Details** button.
- Step 5** On the next screen, provide the details of the SIP Trunk. The following fields are displayed:

Field	Description	Remarks
Trunk Name	The trunk name.	This is a display field only.
Cluster Name	The name of the PBX cluster.	This is a display field only.
Description	A description of the trunk.	-
SIP Profile	Lists the available SIP Profiles to apply to the connection.	Select from the drop-down list
Select SIP Normalization Script	Lists the available Normalization Scripts to apply to the connection.	Select from the drop-down list.
Script Parameters	Key-value pairs to be used by the script.	This is supplied in the format of key=value;key2=value2;key3=value3, e.g. vendor=cisco;pbx;trunk-id=1234
Script Trace Enabled	To enable or disable script tracing.	Select the checkbox to enable script tracing.

- Step 6** Click the **Modify** button.

Note

Click the **Reset Trunk** button to reset the trunk's settings.

Provisioning Other System Features

This section describes how to use the *AutoCCMNewPhone* feature, to move phones between location subnets and to set up the Cisco Unified Communications Manager.

AutoCCMNewPhone Feature

Note

This section assumes that your system is already fully deployed and correctly configured. This includes adding phone types, adding subnets, adding locations and allocating the subnets to the locations.

General Overview

The system includes a transaction called *AutoCCMNewPhone*, this transaction performs multiple functions and is involved with the auto discovery and auto inventory of phones triggered by the *AutoRegister* daemon. Preferences are used within the system to manage the automatic moving and registration of handsets.

This feature enables the system to process phone registration events from Cisco Unified Communications Manager (Unified CM) that are received via the Syslog process. The *AutoReg* service schedules *AutoCCMNewPhone* transactions based on the receipt of a registration event from Unified CM via Syslog.

The initial processing of the Unified CM Syslog message is done by the AutoReg service. This process parses the Syslog message to schedule the AutoCCMNewPhone transactions if required. The information parsed from the Syslog file includes (some vary by version of Unified CM):

- **Node ID:** Generally the CCM server host name
- **Protocol:** Provided in Cisco Unified Communications Manager 5.1 and later
- **Device Name:** The autoregistered device name from Unified CM (SEP + MAC address)
- **IP:** IP address Unified CM knows for the phone
- **Device Type:** This is the phone type reported by Unified CM
- **Device Description:** Description from Unified CM
- **AssociatedDN:** The autoregistered DN number in Unified CM (if available)

The AutoCCMNewPhone transaction supports the following actions:

- AutoInventory
- AutoMove
- AutoRegister
- Update IP Address for a registered phone

The exact actions carried out are determined by the current state of the phone and preferences within the system.

This feature is generally used in environments where the system does not manage the DHCP scopes for phones (unmanaged DHCP, NAT/PAT, etc). This process allows the system to learn the IP Addressing information for phones; this enables the system to provide services to the phones.

Note

- If one of the steps fails, the whole transaction is not rolled back, just the individual transaction. For example, if AutoInventory succeeds but then AutoMove fails, the phone will remain in the inventory of the provider but any changes made during AutoMove will be rolled back.
 - This feature cannot be used to change a phone's subnet - see [Moving Phones between Location Subnets on page 187](#) for more information.
 - The preferences used to manage the AutoCCMNewPhone functionality are hierarchical. Enabling a preference at a lower level (Location) if the same preference is not enabled at a higher level (Customer) will lead to no change within the system. Disabling a preference at a lower level (Location) if the same preference is enabled at a higher level (Customer) will lead to that functionality being disabled at the lower hierarchical level (Location).
-

AutoInventory

If the phone is unknown and the provider preference *Provider.AllowAutoPhoneInventory* is enabled, the AutoInventory process will attempt to add the phone to the system's inventory.

The process determines the provider for the phone by determining the provider of the Cisco Unified Communications Manager (Unified CM) Server sending the Syslog message to the system (this is based on the host name details in the *Node ID* part of the message). The system matches this against the host name of the known Unified CM servers to determine the provider. If this process fails, there is a global setting that will determine the provider (

AutoCCMNewPhoneProvider). If both of these fail or the determined provider does not have *AutoInventory* enabled, an error message is returned that states, "No provider configured for Auto discovery of phone inventory".

After determining the provider, the system will determine the phone type of the phone. The system does this by querying the *Phone Types* (*Product ID* field) and *Protocol* against the *Device Type* and *Protocol* received in the Syslog message. If no match is found, an error will be turned to that effect and the phone will not be added to the inventory.

Note

- As the query checks based on the Product ID field in the system, it is possible for more than one phone type in the system to match. In this case, the first phone type will be used (the query results are listed alphabetically). This is something to note if more than one instance of a Unified CM phone type is configured in the system.
 - This process does not work with the Unified CM in manual mode as the Syslog messages won't be generated.
-

AutoMove

If the phone is not part of a location within the system, the *AutoCCMNewPhone* transaction will attempt to schedule a *MactoLocation* transaction.

During this process, the system attempts to workout which location the phone belongs to, based on the IP address of the phone. The system does this by determining the subnet from the IP address and then checking the location records to see if the subnet is known and assigned to a location. If the system finds the subnet, and it is assigned to a location, the system will check the *AutoMove* preferences (Customer and Location) to determine if AutoMove is allowed. If the preferences are enabled, the *AutoCCMNewPhone* transaction will initiate a *MactoLocation* transaction to move the phone to that location and place it there as an unregistered phone. The most common errors during this process include the preference not being enabled and the subnet of the phone not being tied to a location.

Note

- Ensure in the Cisco Unified Communications Manager (Unified CM) that the phone autoregisters with is the same Unified CM supporting the location in the system. If they are not the same, the system will provision the PBX that supports the location for that phone, however, the phone will still be talking to the Unified CM that it is autoregistered with.
 - If a subnet is tagged as shared in the system, the subnet instance in one of the locations that needs to be selected for AutoMove. This is done when the subnet is added to a location by selecting the *Location used for Automove?* option. AutoMove will move any phones on that subnet to that location. If a subnet is shared and the *Location used for Automove?* is not selected in any of the locations, AutoMove will not proceed. For more details, see: [Manage Subnets on page 762](#).
-

AutoRegister

This part of the process will attempt to register the phone with the next available extension in the location. This behavior is controlled via the location preference *AutoRegister*. Other related preferences also need to be configured for this to work properly, these include *AutoRegisterLowestLocation* and *AutoFeatureLocation*.

Autoregister will leave you with a phone registered with a single line (selected based on the next available line - defined by the preference *AutoRegisterLowestLocation*) and with the feature group determined by the preference *AutoFeatureLocation*. If either of these preferences are not set, errors will be returned by the AutoRegister feature.

If the *AutoRegister* preference is turned off for the location, the phone will remain in an unregistered state within the location. Further registrations can be completed via the GUI, Bulk Loader or via the phone-based Auto Registration processes.

The location preferences setting *AutoDevicePoolLocation* is used to determine the location device pool to use during auto registration and is optional. If this preference has never been set, the location's default device pool is used.

Update IP Address for a Registered Phone

The system compares the IP address it holds for the phone to the one received from the Cisco Unified Communications Manager (Unified CM) Syslog message. The returned IP address will either be the same or different:

- **The IP Address is Different:** If the phone's current IP address differs to the one that the system currently holds for it, the system will update its records based on the new address from Unified CM. If this happens, the result message for the AutoCCMNewPhone transaction will indicate the update.
- **The IP Address is the Same:** If the IP address is the same for the phone as it is in the system, no further action is taken. The resulting message will indicate that the phone was connected to the Unified CM for tracking purposes only.

Note

This step will happen even if the phone is already added to the system.

Moving Phones between Location Subnets

A phone will not move subnets via the *AutoDiscoverIP* workflow. When the phone is moved to a location, the subnet is selected, when the phone is moved, the phone will change IP address but within the same subnet. If the phone's subnet needs to be updated, this cannot be done via the *AutoDiscoverIP* workflow (transaction). To change the subnet, the phone needs to be moved from the location and moved back into it again.

Procedure

In the system, we recommended the following method:

- | | |
|---------------|---|
| Step 1 | Unregister the phone from the location, this will effectively return the device to an unallocated state in the phone inventory. |
| Step 2 | Attempt to autoregister the phone on the new subnet. |
-

Note

The same is also true for a manually setup phone.

Configuring Cisco Unified Communications Manager and the System

The Unified Communications Manager and the system setup are described here.

Cisco Unified Communications Manager (Unified CM) Setup

The first step is to set up the AutoRegistration and the relevant settings in Unified CM. For further details, see the relevant Unified CM documentation for enabling and configuring autoregistration.

The second step in the Unified CM setup is to enable the Syslog messaging from Unified CM to the system. This is done via the alarms configuration in Unified CM. The navigation is slightly different depending on the version of Unified CM, but is found under the serviceability area, *Alarms > Configuration*. Select a server running Unified CM and enable Unified CM alarms to remotely log to the system's virtual cluster address, with the debug level. The alarm level is informational. Select the *Apply to all nodes* checkbox so all Unified CM servers send Syslog.

System Setup

From system release 7.1 onwards, the autoreg process runs as part of the platform and only limited configuration is required. The required configuration includes:

System Level

Procedure

Step 1 While logged in as a super-user, browse to *Setup Tools > Global Settings* .

Step 2 Enable the *AutoCCMNewPhoneProvider* preference.

This preference determines which provider is used by the *AutoCCMNewPhone process* if the provider cannot be determined by the Unified CM details.

Provider

Procedure

Step 1 While logged in at the provider level, browse to *Setup Tools > Global Settings* OR browse to *Provider Administration > Providers > <provider name> > Preferences* .

Step 2 Enable the *ProviderAllowAutoPhoneInventory* preference. This preference determines if AutoInventory is enabled for the provider.

Customer

Procedure

Step 1 While logged in at the customer level, browse to *Setup Tools > Global Settings* OR browse to *General Administration > Customers > <customer name> > Preferences* .

Step 2 Enable the following preferences:

- *AutoMoveCustomer*: This preference determines if AutoMove is allowed for the customer or not.
- *AutoFeatureCustomer*: This preference determines which feature group is used for the AutoRegister process.
- *AutoRegisterLowestCustomer*: This preference determines where the extension allocation for the AutoRegister process begins. The logic will start at this number then find the next available unallocated number.

Location

Procedure

- Step 1** While logged in at the location level, browse to *Setup Tools > Global Settings* OR browse to *General Administration > Locations > <location name> > Preferences*.
- Step 2** Enable the following preferences:
- **AutoMoveLocation:** This preference determines if AutoMove is allowed for the location or not. If the AutoMoveCustomer preference is not enabled, enabling the AutoMoveLocation preference will have no impact on the system. However, disabling the AutoMoveLocation preference while the AutoMoveCustomer preference is enabled will disable AutoMove for the selected location.
 - **AutoFeatureLocation:** This preference determines which feature group is used for the AutoRegister process. If the AutoFeatureCustomer preference is not enabled, enabling the AutoFeatureLocation preference will have no impact on the system. However, disabling the AutoFeatureLocation preference while the AutoFeatureCustomer preference is enabled will disable the AutoFeature functionality for the selected location.
 - **AutoRegister:** This preference determines whether phones can be AutoRegistered in the location via the AutoCCMNewPhone transaction.
 - **AutoRegisterLowestLocation:** This preference determines where the extension allocation for the AutoRegister process begins. The logic will start at this number then find the next available unallocated number. If the AutoRegisterLowestCustomer preference is not enabled, enabling the AutoRegisterLowestLocation preference will have no impact on the system. However, disabling the AutoRegisterLowestLocation preference while the AutoRegisterLowestCustomer preference is enabled will disable the AutoRegisterLowest functionality for the selected location.
-



CHAPTER 2

Key System Functionality

Add Users and Services 199

Adding End Users and Adding (Associating) the Required Services/Devices 199

Important Points to Know About Users and Services 199

Pre-requisites 200

Using the GUI 200

Using the Bulk Loader 201

Related Topics 202

IOS Gateways 202

IOS Device Management 205

Adding an IOS Device 205

Modifying an IOS Device 208

Device Roles 209

Media Service Management 264

Configure Per-Port COS for Emergency Calls from Analog Ports 264

Activate Per-Line COS for Analog Gateways 265

Supplementary Services on Analog Gateways 266

Enabling Supplementary Services 266

Analog Port Management 268

Register an Analog Line with an Analog Port 271

SCCP Supplementary Features 272

Valid Analog Line Features 272

Key Sync Features 273

IOS Commands 273

Download Command List 284

Exporting IOS Commands 284

PGW Pre and Post Functions 289

Supported MML Scripts 289

Transaction Failures and Rollback 289

Legacy Gateways	290
Search Functionality	290
Adding an IOS Device	290
Location Local Gateway Provisioning	301
The Local Gateway Index	301
Initial Provisioning of Dial Plan	301
Modification of the Current Dial Plan	302
Activation of Additional Ports/Gateways	303
Deactivation of Ports	303
Removal of Dial Plan	304
Transit Switch Management	304
PGW Server Management	306
HSI Management	312
Transit/Transit Server Management	318
Transit/Voicemail Server Management	319
Transit/Gatekeeper Management	320
Transit/IPPBX Server Management	321
PBX Server Management	322
IPPBX/Gatekeeper Management	323
IPPBX/Transit Management	324
IPPBX/Emergency Responder Server Management	325
IPPBX/Conference Management	326
IPPBX/Transcoder Management	327
IPPBX/TFTP Management	328
IPPBX/Voicemail Management	329
IPPBX/Third Party SIP Management	330
IPPBX/Location Management	331
Call Routing Connections	332
IPPBX/Contact Center Management	346
Device Sets	347
Connecting an Unmanaged Legacy PBX to another PBX	349
TDM Connectivity via an MGCP Gateway from a Leaf Cluster	349
IP Connectivity using H323 Trunks from a Leaf Cluster	351
IP Connectivity using SIP Trunks from a Leaf Cluster	351
Call Routing	352
Defining Call Routing Types in the system	352

Associate Call Routing Types to Country	352
Applying Call Routing at Location Level	353
Local Gateway Port Call Routing	354
Bulk Loader and Model Loader Changes	355
The Survivable Remote Site Telephony (<i>SRST</i>)	355
SRST Role	355
NAT for Gateways	359
NAT of Gateway Address to Unified CM	360
NAT of Unified CM Address to Gateway	360
Guidelines for usage based on specific NAT configuration	360
PGW Export Tool	361
Supported Transactions	361
Activating the PGW Export Functionality	362
Exporting MML and Times Ten data	362
AssociateFNN	363
Cloned Line (Multiline) Functionality	364
Support for Cisco Analog Telephone Adaptors (ATA)	368
Support VIA SIP	368
Mobility Connect	369
Versions	370
Required Plug-ins	370
Configuring Mobility Phone Type Integration	370
Eventing	370
Licensing	372
Enabling/Disabling License Types	372
Viewing Available Licenses	374
Refreshing the <i>Location License Management</i> page	374
Requesting a Quote For License Updates	374
Submitting an Order	375
Meet-Me	376
Adding a Meet-Me Number	376
Managing a Meet-Me Number	377
Bulk Loading Meet-Me Numbers	377
Managing Phone Services	378
Enabling IP Phone Services in a Feature Group	382
IP Phone Service subscription management	383

Modify container details	383
IP Phone Service Subscription Management for Individual Devices	384
Manage IP Phone Service Subscriptions	385
Leaf Cluster Overview	386
PBX to PBX Connection management	387
SME Clusters	392
Cisco Unified CM Session Manager Edition	392
Managing SMEs via Bulk Loaders and Models	392
Managing SMEs via the system GUI	392
Idle URL Management	400
Adding a Service Type for an Idle URL	400
Managing the Idle URL Setting via the Feature Group	401
Managing the Idle URL Individually for the Phone	401
Extension Mobility Cross Cluster (EMCC) Configuration	401
EMCC Use Case	402
EMCC Server Setup	402
Home Cluster Setup	403
View EMCC Configuration	412
EMCC Group Management	413
Enabling/Disabling EMCC using the Bulk Loaders	415
Extension Mobility Location Group Management	415
Adding an Extension Mobility Location Group	416
Modifying an Extension Mobility Location Group	416
Mobile Connect/Single Number Reach (SNR)	417
Adding a Single Number Reach Remote Destination	418
Setting and Resetting a Primary Device for an End User	424
Modifying a Single Number Reach Remote Destination	425
Checking the CCM Data	425
Mobile Identity Management	425
Synchronization with Cisco Unified Communications Manager (Unified CM)	429
Subnets	429
NAT and PAT	430
Adding and Managing Subnets	430
Edge Devices	431
Extension Management	431
Managing Available Internal Numbers	431
Manage Extensions (Internal Numbers) using Bulk Loaders	432

- Connect Location **432**
 - Via the *Location Administration* Menu **432**
 - Via the *Operations Tools* Menu **433**
 - Associate PSTN Number Ranges and Connect Location **434**
- Feature Display Policies **434**
 - Adding a Feature Display Policy **435**
 - Adding Feature Display Policy Groups **437**
 - Feature Display Policy Management **438**
 - Assigning Feature Display Policies **438**
- Shared SLC **439**
 - Adding a Linked Location Parent **440**
 - Converting a Standard Location to Linked Location Parent **440**
 - Converting a to Linked Location Parent a Standard Location **441**
 - Adding a Linked Location Child **441**
 - Reassigning the Linked Location Parent Role in Linked Locations **441**
 - Hunt Group/Number Groups for Linked Location **441**
 - Location Level Operations Tool to Delete Lines of Different Linked Location from the Number Group **442**
 - Bulk Loading Linked Locations **442**
- CTI/TAPI Management **442**
 - Adding CTI Route Points/ CTI Ports **442**
 - Line Setting Information **445**
 - Modifying CTI Route Points/ Ports **451**
- Transit Deferral **452**
 - Enabling Deferral **452**
 - Error Handling **452**
 - Affected Transactions **453**
- Session Border Controllers **453**
 - Session Border Controller Management (SBC) **453**
 - Manage Session Border Controller **455**
 - SBC Connected Locations **458**
 - Manage SBC Interfaces **459**
 - SBC Connectivity **461**
 - Allocating Location to the Hardware **463**
- SBC and OCS Management **463**
 - Activating an SBC **463**
 - Deactivating an SBC **464**

Modifying the Call Limit and OCS Numbering	464
Access Profiles	465
Additional Restrictions	467
Adding an Access Profile	470
Modifying and Deleting Access Profiles	475
Defaults for Access Profiles	475
Security profiles	489
Security profile management	489
Adding a security profile	490
Modifying and deleting security profiles	493
Brand Management	494
Importing a Brand	495
Brand Editor Overview	496
Deploying Brands	498
Feature Group Administration	500
Feature Group Management	500
Features Available when Adding or Modifying a Feature Group	505
Device Group Management	513
Operations Tools	515
Transaction Log and Search Report	515
Using the transaction search screen	515
Access to Transaction Logs for End Users	516
Bulk Administration	516
Bulk Administration Preview and Add	518
Bulk Administration file formats	520
Common Bulk Administration tasks	520
IVR/Transit Server Management	525
Transaction Auditing	526
Management of Transaction Auditing	526
Transaction Auditing Application	528
Transaction Details	529
Billing Codes (Client Matter Codes)	530
Quick Search	534
Search For	534
Finding Locations	535
Finding Extensions	536
Finding Phones (Device Name)	538

Phone with Extension	539
Phone with DDI	539
Phone with User	539
Find a Phone in the List	539
Finding a User	541
Bulk and Model Loader Functionality	543
Model Management	543
iFINT Migrate Feature	549
Number Construction Rules	549
Activating the iFINT Migrate Functionality	549
iFINT Migration History Logs	550
Dial Plan Terms	550
Number Construction	551
Details	551
Codec Selection	551
Dial Plan Rules	551
Internal Number Format	552
Internal Number Display Rules	553
RID Type Selection	553
Dial Prefixes	553
Format of External Phone Number Mask on Unified CM	554
Format of IPPBX Configured Internal Number	554
Format of Voicemail Configured Pilot Number	555
Format of Voicemail Configured Mailbox Number	555
Configurable FINTs	556
Recommended Dial Plan Configuration by Solution	556
HCS Solution	556
Device Pool Templates	558
Adding a Device Pool Template	559
Modifying a Device Pool Template	561
Feature Configuration Templates	562
End User Migration	563
End User Migration Preview	565
Number Translations	565
E164 Numbers	570
Pre-requisites for adding E164 numbers	571
Using the GUI	572

Using Bulk Loaders	579
Related topics to E164 numbers	580
Forced Authorization Codes	581
Add FAC	582
Assign FAC	583
Release FAC	583
Delete FAC	583
Customer Specific Button and Softkey Templates	583
Button Group Management	583
Emergency DDI	587
Country Setting	587
Customer Setting	587
Location setting	588
FNN Range Setting	588
Authentication Management	588
Enable External Authentication in Security Profile	589
Authentication Management steps	590
LDAP Integration with Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection	594
Limitations	594
Configuring LDAP Integration	595
Cisco Unified Communications Manager IM and Presence (IM and Presence) Server	603
Managing a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server	603
Connect an IM and Presence Server to an IPPBX	607
Cisco Unified Communications Manager IM and Presence (IM and Presence) Manual Configuration	608
Driver_Presence Implementation of the <i>VerifyCUPCapabilities</i> Transaction	610
Service Profile Management	610
UC Central	618
Provisioning UC Central	619
Enabling a User's extension as a UC Central extension	623
Disabling a User's extension as a UC Central extension	624
Deactivating a User's UC Central connection	624
Voicemail Services Management	624
Add a Voicemail Service	625
View or Delete a Voicemail Service	625
Conferencing	626

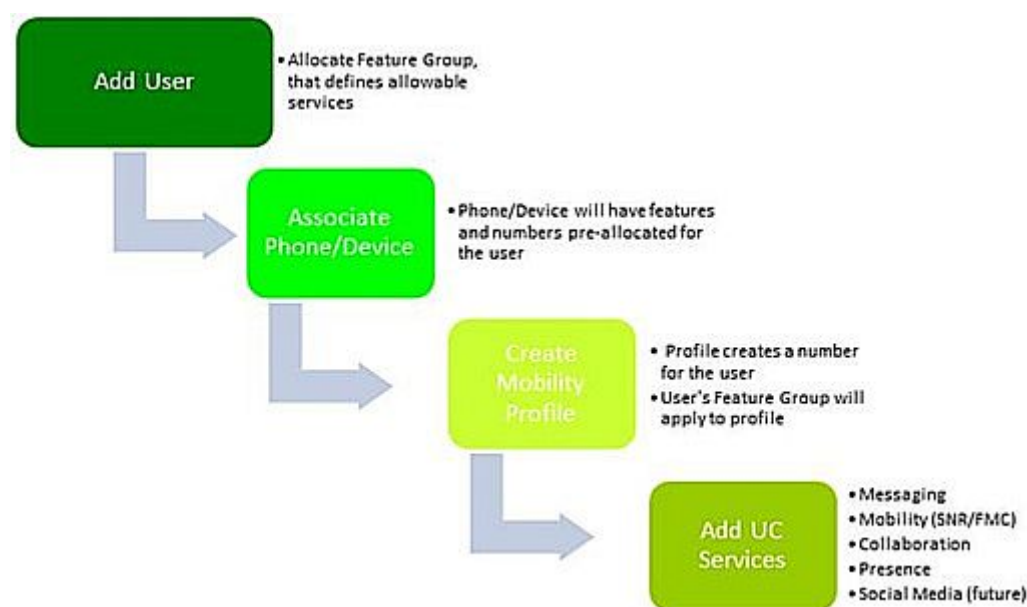
- Conference Service Management **626**
 - WebEx Conferencing **633**
- Single Inbox **637**
 - Activating Single Inbox **637**
 - Selecting a Unified Messaging Service for Single Inbox **638**
 - Modifying the Unified Messaging Service for an Existing Voicemail Account **638**
- Corporate Directory Partitions **638**
 - Assigning a Directory Partition **640**
- Hide a Shared line from Corporate Directory **640**
- CLI Group Management **641**
- Codecs **646**
 - Default Cisco Unified Communications Manager (Unified CM) Codec Values **647**
 - Audio Regions **647**
 - Bulk Loading Codecs **649**
 - Automatic Codec Scaling **649**
- Contact Centers **650**
 - Contact Center Servers **650**
 - Contact Center Service Management **654**
 - Recording Profiles and Recording Options **661**
 - Migration Concerns **662**
 - Service Inventory: Billing **662**
 - Caveats **662**
- ASCII Fields **662**
 - Enabling ASCII fields in the Feature Display Policy **663**
 - Enabling ASCII fields in the Feature Group **663**
 - Phone Lines **663**
 - CTI Route Points **664**
 - CTI Route Ports **664**
 - Mobility **664**
 - Busy Lamp Fields **665**
 - Speed dials **665**
 - Bulk loading ASCII values **666**
- Importing Device Specific Settings **666**
 - Importing Advanced Phone Features **666**
 - Feature Group setting for Advanced Phone Settings **668**
 - Feature Display Policy Setting for Advanced Phone Settings **668**
 - Managing Advanced Phone Settings for a Device **668**

Managing Advanced Phone Settings in Self Care	669
Specifying Advanced Phone Settings when Bulk Loading Phones	669
Importing Advanced Phone Settings for Existing Devices via CLI	669
Music on Hold Track Management	669
Adding a MoH Track	669
Viewing and Modifying MOH Tracks	670

Add Users and Services

This section provides a brief description of the end-to-end process flow for adding users and their associated devices and services. Associated cross-references to related documents are also provided. The section is aimed primarily at administrators, and describes how to add an end user to a specific location and then associate the relevant devices and services to those users. Refer to Figure 1 below for a diagram that illustrates the process of adding users and services.

Figure 1. Add users and services process diagram



Adding End Users and Adding (Associating) the Required Services/Devices

This section describes the process of adding an end user. It then describes how to activate (allocate) the required services/devices to the end user as a function of their service profile (or feature group).

Adding end users, their required devices, their required mobility profiles, and their required services can be done using either the GUI or by using a bulk loader.

Important Points to Know About Users and Services

Before adding users and allocating their services/devices, take note of the following important points:

- **User names must be unique.** User names must be unique across the entire platform. The user name must be in lower case and can only contain ASCII characters. You should establish a naming convention (such as first name, last name, company name, or the primary E164 number for the user) to ensure uniqueness.

- **Feature Groups.** A service, e.g. Voicemail, Presence, Single Number Reach, etc. can only be activated for a user if the service is available and enabled within their allotted Feature Group.

Pre-requisites

Before adding an end user, the following processes (see table below) must be performed in the sequence provided.

Table 1. Pre-requisites for adding an end user

Step	Brief Description / Remarks	Detailed Information (Where?)
1.	Feature Groups - make sure that the required feature group(s) is available for association with the end user.	See <i>Feature Group Management</i> and <i>Adding a Feature Group</i> in Feature Group Management on page 500 .
2.	Access Profile - make sure that the required access profile has been added to the system. Note The <i>Default</i> access profile option in the drop-down list is automatically provided by the system.	See Access Profiles on page 465 and Adding an Access Profile on page 470 in the Deployment Guide.
3.	UC Services - make sure that UC services have been created at the Customer and Location levels. This is completed as part of the Add Customer and Add Location processes - refer to the Deployment Guide if necessary.	See also table of other services on page 201 .
4.	Phones and devices - make sure that phones and devices have been added to the Location.	See the <i>Add Phones Process</i> guide.
5.	Numbers - make sure that numbers have been added to the Location.	See E164 Numbers on page 570 .

Using the GUI

Perform the processes (see below) in the displayed order.

No.	Process	Cross-reference	Remarks
1.	Adding an End User	Add an End User on page 842 .	This process adds a user account with an end user role to the system's database, and links it to the location in which the administrator is currently operating.
2.	Associating Devices to an End User	Associate/Unassociate (or Delete) Device with/from User on page 852 .	This process associates a device (phone or analog line) with an end user account, configures the device and links it to the end user.
3.	Associating an Extension Mobility Profile to an End User	Adding an Extension Mobility Profile on page 863	Extension mobility profiles enable a user to log onto a phone in another location and the phone automatically adopts the profile for that user.
4.	Adding Other Required Services to an End User	See table of other services on page 201 .	A feature must be allowed/enabled within the feature group to which the end user is allocated in order to activate it for the end user.

Service	Detailed Information (Where?)
Single Number Reach. Enables an incoming call to a corporate phone to be directed to the user's normal desk phone as well as up to ten other configurable destinations	See Mobile Connect/Single Number Reach (SNR) on page 417 and Adding a Single Number Reach Remote Destination on page 418 for details.
Presence. Brings people together in and across organizations in the most effective way. This open and extensible platform facilitates the highly secure exchange of availability and instant messaging (IM) information between Unified CM and other applications.	See Managing a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server on page 603 for general information about Cisco Unified Presence. See under " To Configure a User for Unified Presence " for the procedure on how to configure a user for Presence.
Voicemail. Enables callers to leave messages for the user when a phone is unanswered or diverted to the Voicemail system and the User can then retrieve the message when he/she is available.	See Manage Voicemail Accounts on page 867 .
Conference. Enables two or more users to participate in a conference call.	See WebEx Conferencing on page 873 .
UC Central. An enterprise tool used to deliver voice, web and video conferencing capabilities to end users.	See UC Central on page 874 .
Mobile Identity. Enables an incoming call to be directed directly to a remote destination.	See Mobile Identity Management on page 425 .

Using the Bulk Loader

Step 1: Adding End Users

A bulk loader can be used to expedite the process of adding end users to the required location.

See the *Add End Users* sheet under the relevant *LocAdmin* spreadsheet in the Bulk Loader Guide for details. Each row on the spreadsheet represents a new user and each column specifies a user.

Step 2: Associating Devices to an End User

A bulk loader can be used to expedite the process of adding devices to an end user.

See the *Associate User Device* sheet under the relevant *LocAdmin* spreadsheet in the Bulk Loader Guide for details.

Step 3: Associating an Extension Mobility Profile to an End User

A bulk loader can be used to expedite the process of associating an extension mobility profile to an end user.

See the *Add User Mobility* sheet under the relevant *LocAdmin* spreadsheet in the Bulk Loader Guide for details.

Step 4: Adding Other Required Services to an End User

A bulk loader can be used to expedite the process of adding other required services to an end user.

See the relevant sheet listed below in the *LocAdmin* spreadsheet in the Bulk Loader Guide for more information

- Single Number Reach: Add Single Number Reach

- Presence: Presence Clients
- Voicemail: Add User Voicemail
- Conference: Add User Conference Account
- UC Central: N/A
- Mobile Identity: Add Mobility ID

Related Topics

Telephony Groups

After adding an end user to the system, the user can be added to a particular telephony group as required:

- **Pickup Group.** See [Pickup Groups on page 905](#) and [Adding a Pickup Group on page 906](#).
- **Hunt Group.** See [Hunt Group Management on page 901](#) and [Adding a Hunt Group on page 902](#).

Deleting UC Services from a User

Service can generally be deleted from a user via the User Management screen of the specific end user. Select the required Username link (active text link), and then click the relevant button of the previously added service, e.g. Single Number Reach, and then click the **Delete** button. In some instances you may have to click the *Y* link (active text link) adjacent to the service.

Un-associating (Disassociating) Devices from an End User

To disassociate a device from an end user is almost the same process as explained under [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#), except you must click the **Un-Associate** button on the relevant *Associate Device* screen.

Replacing a Phone

See "Replace a Phone" in [Managing the Phone on page 806](#).

IOS Gateways

The IOS device and gateway functionality within the system has changed significantly from previous versions of the system. This section will give an overview of the functionality currently supported in the product.

The rationale behind the IOS device and gateway management is that an IOS device can actually perform many roles. These additional roles may be added to the product over time and the gateway functionality is the first to be included. The overall general logic is that you would add an IOS device, add functions to that device (e.g. Gateway), then have specific configuration steps as required for that function.

Once the IOS device is added, a gateway instance can be added to it. This will involve a workflow to add the gateway details including roles, configure the hardware settings, add and configure the interfaces, and allocate them to specific role and level in the hierarchy. There are also additional location level dial plan activation steps depending on the role of the gateway. Multiple gateway instances can exist on a single IOS device depending on the requirements and protocols being used (e.g. a MGCP and H323 gateway). This multiple instance is restricted to one per protocol.

Each gateway instance needs to be connected to the required call agent. This is based on the protocol select but will be either an IPPBX or Transit device. MGCP and SCCP gateway instances

are restricted to a single call agent, while H323 can be connected to multiple call agents if required.

A gateway instance can provide multiple roles (e.g. Local Breakout and analog), while an individual port on the gateway can only be allocated a single role. The roles available depend on the protocol and the call agent the gateway is connected to.

Important Information

Please take note of the following important information:

- Shared buildings are not supported by local gateways.
- The `tunneledProtocol` parameter used with H323 Gateways is not supported in Cisco Unified Communications Manager (Unified CM) 6.1 and Unified CM 5.1. If using a Unified CM 6.1 or Unified CM 5.1, please configure this setting manually on the Unified CM.
- The SIP protocol is supported from Unified CM version 6.1. and higher.
- `DTMFSignalingMethod` is not supported by the system for Unified CM 6.1. If using a Unified CM 6.1, please configure this setting manually on the Unified CM.
- SRST is supported on H323 and SIP gateways.
- The voice service VoIP command is currently not supported by the system. Please run this command manually if you require it. This issue is caused by known Telnet Limitations and may affect certain other commands as well (see [IOS Commands on page 273](#)).
- Unified CM versions 6.1 and earlier do not support the `<digestUser>` tag. The result is that if Unified CM 6.1, or earlier, is being used, the system will not be able to set the digest user for the phone.
- The IOS device IP address can be changed at any time. The gateway IP address is however locked once the hardware configuration is setup (i.e. the Gateway has been loaded into the PGW). The IOS device IP address remains configurable as this isn't the IP address used in the call agent.

Available Hardware Setup and Configuration Options

The system provides the following gateway functionality:

- IPPBX Connected Gateways supporting H323, MGCP, SIP and SCCP
- Cisco Unified Communications Manager (Unified CM) connected MGCP and SCCP hardware setup based on Unified CM data as all these details are required to add via AXL (e.g. Chassis, slots, modules, etc).
- Transit Connected MGCP Gateways
- Ability to have multiple Gateway instances per IOS device
- Transactions to provision the Call Agent (Unified CM or Transit) as well as the IOS Device with the required hardware and port configuration.
- Multi-level hierarchy access to the IOS device management screens - based on the owner of the device.
- Wizards for select setups to streamline to addition of the gateway and configuration.

Local PSTN Gateways

This role involves a gateway being allocated to a single location and used for local PSTN breakout:

- Supported for IPPBX connected MGCP, H323 and SIP gateways
- Any number of Local gateways per location
- Local Gateway role is dedicated to a single location
- Additional Location level dial plan management for Cisco Unified Communications Manager and IOS device
- Supports ISDN PRI (E1/T1), ISDN BRI, and FXO port types.
- No differentiation of call routing for specific call types via the system (Central vs. Local)
- IOS Hardware config, port config, and POTS dial peers and such are model driven

Analog Gateways

This functionality replaces any previous analog gateway functionality in the system. This role involves a gateway being allocated to a location and the FXS ports used for analog device connectivity (old phones, fax, modem, etc).

- Supported for IPPBX connected MGCP, H323, SIP and SCCP gateways.
- Only FXS ports can be assigned to this role.
- Any Cisco Unified Communications Manager IOS device included in the MGCP/SCCP data should be supported. For H323 anything is supported as chassis details are not required.
- Analog Gateway dedicated to a single location
- H323 and SIP gateways do not support per port Calling Search Space (CSS) natively, as ports on MGCP and SCCP gateways do, which means the CoS (CSS) is applied on the gateway level so all ports have the same CSS. This limitation can be overcome by enabling the per-port CSS (COS) feature which allows the assignment of a COS (CSS) per port thereby overriding the gateway CSS (COS).
- Support for any DTMF based features (i.e. start codes) are supported depending on model setup.
- IOS Port and hardware configuration (and dial peer for H323) is model driven.

Legacy Gateways

This functionality replaces any previous analog gateway functionality in the system. This role involves a gateway being used to provide connectivity between the IP network and a legacy PBX(s).

This is generally used for migration purposes or links to devices requiring non-IP connectivity:

- Supported for Transit Connected MGCP based gateways
- Support for E1 and T1 interfaces
- Support for DPNSS and Q931 legacy protocols
- No limit to the number of gateways for a location
- Gateway allocated to a Location - cannot be shared between locations
- Support for Unmanaged locations only (not hybrid managed/unmanaged)
- Additional Location level dial plan management for Transit

SRST

This covers the provisioning of the Cisco *SRST* capability for backup of telephony in the case of WAN failure.

- Supported on H323 and SIP gateways.
- No limit to number of gateway per location
- Phone management selection of SRST gateway to use
- Configuration of SRST reference and device pool in Unified CM (except for version 4.2)
- Configuration of IOS device based on models

For more information on *SRST* functionality, see under [The Survivable Remote Site Telephony \(SRST\) on page 355](#).

IOS Device Management

This feature allows a user to add, modify and delete an IOS Device with the associated device roles such as a Gateway, Media Resource or SRST. It also allows for country specific information to be associated with a device via the country code.

This functionality is accessed by browsing to *Network > IOS Devices*.

Note

If a transaction fails on an IOS device at any point, the IOS device configuration up until the point of failure remains on the IOS device. This configuration must be removed manually from the IOS device before running the same transaction. For example, if MTP is added with incorrect codecs from CUCDM, the transaction will fail but the profile will remain on the device. This profile must be removed manually from the IOS device before attempting to add MTP.

See also: [Adding an IOS Device on page 205](#).

See also: [Modifying an IOS Device on page 208](#).

Adding an IOS Device

An IOS Device is effectively a placeholder to contain either Gateway, Media Resources or SRST device role configuration in Cisco Unified Communications Domain Manager (CUCDM). Provisioning is done via Telnet or SSL to the configured IP address and user credentials in CUCDM. A prescribed IOS model is sent to the device for configuration during addition of device roles. The following device roles are supported:

- Media Resources
- Gateways
- SRST

Note

IOS Devices with Gateways can also be added via the IOS Gateway Wizard. For information on adding IOS gateways using the wizard, see [IOS Gateway Wizards on page 221](#).

Procedure

To add a custom IOS device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button.

Step 3 Click the **Custom Add** button.

Step 4 Complete the required fields (see table below for details).

Field	Notes	Remarks
Device Details		
Host Name	The host name of the IOS Device.	This is a mandatory field.
Description	Description for the device being added.	-
Country	The country specific details to be applied to the device.	This is a mandatory field. The default country is the country of the current provider. The list of available countries will be filtered according to the countries available to the provider.
Select Owner	Configured ports may only be allocated to locations that fall within the owner, thus this field is used to control who can access the device for management purposes (updating settings, adding/configuring, and so on). If the owner is a provider (default), only the provider administrator and above can access the IOS device via the system's Network menu. If this is set to a location level, the location administrator for that location (and higher level administrators) can access the IOS device via the system's Network menu.	This is a mandatory field, and defaults to the current provider.
Select Location	Select the required location from the drop-down list.	This is a mandatory field.
Connectivity Details		
IP Address	The IP address for the IOS device.	This is a mandatory field, and must be a unique IP Address within the provider. Note The IOS device IP address can be changed at any time as this is not the IP address configured into the PGW, the gateway IP is used for the PGW.
IP Address (alternate)	An alternate IP address for the IOS device.	This must be a unique IP Address within the provider.
IP Domain	The domain within which the IP address falls.	-
Cisco User Id Required	Select this checkbox if you would like the IOS device to require a Cisco User ID when accessed.	-

Field	Notes	Remarks
Config User Name	The user name of the person who will be managing the IOS device.	-
Config Password	The password is required to transfer the configuration to the IOS device	This is an optional field if the Manual Configuration Mode is enabled.
Enable Password	The password (re-entered for confirmation) for the Config user as described above.	This is an optional field if the Manual Configuration Mode is enabled.
Software Version	The software version that the device will be running.	-
Manual Configuration Mode	Select this checkbox if you would like the IOS device to be manually configurable. Commands sent to the IOS device will still be logged and can be accessed via the normal set of IOS Command screens.	Note If this option is enabled, it is mandatory to supply an email address.
Email address for Manual activation	The email address used during the manual activation of the IOS device.	This must be entered in the traditional email address format, for example test@example.com. Note This is a mandatory field if the Manual Configuration Mode is enabled (see field above).
Network Monitoring active	Select this checkbox if you would like to activate Network Monitoring on the IOS device.	-
Detailed trace file of configuration sessions	Select this checkbox if you would like to maintain a detailed trace file of all IOS device configuration sessions.	-
Encrypt configuration sessions	Select this checkbox if you would like to encrypt configuration sessions with the IOS device.	We recommend encrypting configuration sessions, however, depending on the setup of your network, a reduction in configuration session performance may be experienced.
Device Roles Note Roles can be assigned to an IOS Device either during the 'Add' process (continue with this procedure) or during the 'Modify' process.		
Gateway	Select this checkbox to assign a Gateway role to the IOS device. After the IOS device has been added, this section lists all available gateways. To add a gateway, click the Add button. To modify a gateway, select the gateway's <i>Name</i> (active text link).	For more information, see Adding a Gateway Role to the IOS Device on page 209 .

Field	Notes	Remarks
Media Resources	<p>Select this checkbox to assign a Media Resource role to the IOS device.</p> <p>After the IOS device has been added, this section lists all available Media Resources. To add a Media Resource, click the Add button. To modify a Media Resource, select the Media Resource's <i>Name</i> (active text link).</p>	For more information, see Adding a Hardware Media Resource on page 258 .
SRST	<p>Select this checkbox to assign a SRST role to the IOS device.</p> <p>To add a SRST role, click the Add button. To modify an existing SRST, select the SRST <i>Name</i> (active text link).</p>	For more information, see SRST Role on page 355 .

Step 5 Select the device roles that are applicable for this device.

Step 6 Click the **Add** button to add the new IOS device. The IOS device is added to the system.

Modifying an IOS Device

Procedure

To modify an IOS device:

Step 1 Browse to *Network > IOS Devices*.

Step 2 Select the *IOS Device*.

Step 3 **Note**

See the Device Roles section in the above table for more details about device roles if required.

Make the required modifications and click the **Modify** button.

Procedure

Delete an IOS Device

To delete an IOS device:

Step 1 Browse to *Network > IOS Devices*.

Step 2 Select the *IOS Device*.

Step 3 Click the **Delete** button to remove the IOS Device.

Note

The **Delete** button is not visible if there are any roles defined and configured for the device.

Device Roles

Procedure

To add a role to an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *IOS Device* (active text link).
- Step 3** Click the **Add** button next to the device role (Gateway, Media Resources or SRST).

Gateway Role

Before assigning a Gateway role to an IOS Device, take note of the information provided under [IOS Gateways on page 202](#).

Adding a Gateway Role to the IOS Device

The Gateway function essentially a role of an IOS device, and is effectively a network point that acts as an entrance to another network.

Router PSTN connectivity is generically referred to as voice gateway functionality, offering a gateway for voice over IP (VoIP) calls to, and from, traditional analog or digital PSTN or private branch exchange (PBX) calls. You can use a voice gateway to connect to PSTN central office (CO) switches, private branch exchanges (PBXs), Key Systems, time-division multiplexing (TDM)-based interactive voice response (IVR) systems, traditional TDM-based voice mail systems, and any other legacy (non-IP) voice processing or telephone equipment.

The following gateway protocols are supported:

- MGCP
- SCCP
- SIP
- H323
- MGCP-DPNSS
- MGCP-Q931

The following gateway port types are supported:

- FXS
- FXO
- E1
- T1
- PRI
- E&M
- BRI

Gateways can have the following functions:

- Analog
- PSTN Local

- Legacy
- PSTN Central

Gateway roles can be added manually or via the Gateway Wizard. For information on adding gateway roles using the wizard, see [IOS Gateway Wizards on page 221](#).

Procedure

To add a Gateway role to an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Device* (active text link) to which you want to add a Gateway role.
- Step 3** Select the *Gateway* checkbox in the *Device Roles* section of the screen.
- Step 4** Click the **Add** button adjacent to the *Gateway* device role in the *Device Roles* section. Mandatory fields include:

Field	Notes	Remarks
Device Details		
Host name	For information purposes only.	Cannot be modified.
Description	For information purposes only.	Cannot be modified.
Single Location Only	For information purposes only.	Cannot be modified.
Location	For information purposes only.	Cannot be modified.
Gateway Details		
Name	The name of the Gateway role.	This is a mandatory field.
Description	Description of the Gateway role.	-
IP Address	This is the IP address used to configure the Gateway itself and could be different to the IP address defined on the IOS device screen (often it is the same).	<p>This is a mandatory field.</p> <p>Note</p> <ul style="list-style-type: none"> • If the Provider preference setting <i>AllowDuplicateIpAddresses</i> is enabled (see Available Preferences and Settings on page 934 if required), a Gateway role can share its IP Address with another Gateway role (as long as the other Gateway role is within a different Customer). • The gateway role IP address is locked and may not be modified once the hardware configuration is setup (that is, the Gateway has been loaded into the PGW). The IOS device and gateway role IP addresses may be different and the IOS device IP address remains configurable as this isn't the IP address used in the call agent.

Field	Notes	Remarks
IP Address (Alternate)	An optional, alternate, IP Address within the provider.	-
IP Address B	This is the IP address that other devices, for example Unified CMs, use when communicating with the Gateway. The use of this field is described by the option that follows.	This is a mandatory field when the <i>Unified CM to use Gateway IP B</i> option is selected. Note This IP Address needs to be provided in the standard IP address format.
Unified CM to use Gateway IP B	This causes Unified CMs communicating with this device to use the IP address configured in <i>IP Address B</i> on the Gateway.	Note This option allows communication from the Unified CM to the Gateway via a NAT Boundary. Details on how to utilize this in a specific scenario are described in the <i>IOS Gateways Guide</i> .
Gateway to Use Unified CM IP B	This Gateway uses the Unified CM IP address configured in the <i>IP Address B</i> field on the Unified CM configuration screen.	Note This option allows communication from the Gateway to the Unified CM via a NAT Boundary. Details on how to utilize this in a specific scenario are outlined in the <i>IOS Gateways Guide</i> .
<i>Protocol</i>	The protocol for the gateway.	This is a mandatory field. The IOS Device may be configured with multiple gateway roles but is limited to one gateway role per protocol.
<i>Supplementary Services</i>	Supplementary Services, including voicemail, call forwarding, conferencing and speed dials can be enabled to be managed at location level as analog line features.	Only available for SCCP analog gateways. Select to enable.

Step 5 Click the **Next** button.

Section	Field	Remarks
Gateway Details	Type and name of the device to which the gateway connects.	Select the type and name of the device to which the gateway connects.

Step 6 Click the **Next** button.

Step 7 Within the *Gateway Functions* section, select the required functions of the gateway (see table below for supported gateway functions).

Protocol	Connect Device Type	Gateway Functions			
		PSTN Central	PSTN Local	Analog	Legacy

Protocol	Connect Device Type	Gateway Functions			
<i>MGCP</i>	IPPBX	Y	Y	Y	
	Transit Switch				Y
<i>SCCP</i>	IPPBX	Y		Y	
<i>H.323</i>	IPPBX	Y	Y	Y	
<i>SIP</i>	IPPBX		Y	Y	

Step 8 Click the **Add** button.

Supported Gateway Functions

SIP Gateways

When using the SIP protocol, please take note of the following:

- The *SIP* protocol is only supported on CCM 6.1. and CCM 7.1
- The *DTMFSignalingMethod* setting is not supported by the system for CCM6.1. If using a CCM 6.1, please configure this setting manually on the CCM.
- The *SIP* protocol only supports *FXS* type ports
- Only one *SIP Gateway* may be added to each device
- When adding a *SIP Gateway*, the only Gateway Function that may be selected is *Analog*.

SIP gateways are configured in the system via the *SIP Gateway Configuration* page.

Procedure

Follow these steps to configure a SIP gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Complete all of the required fields and click the **Submit** button.

The gateway will be configured.

The following fields are available when configuring a H.323 Gateway:

Field	Description	Notes
Device Information:-		
<i>Name</i>	Name of the device currently being modified.	This field cannot be updated via this page.
<i>Description</i>	Description of the device currently being modified.	This field cannot be updated via this page.
<i>Protocol</i>	Protocol of the device currently being modified.	This field cannot be updated via this page.

Field	Description	Notes
<i>IP Address</i>	This is the IP address used to configure the Gateway itself and could be different to the IP address defined on the IOS device screen (often it is the same).	This field cannot be updated via this page.
<i>IP Address (alternate)</i>	Alternate IP Address of the device currently being modified.	This field cannot be updated via this page.
<i>IP Address B</i>	This is the IP address that other devices, for example Unified CMs, use when communicating with the Gateway.	This field cannot be updated via this page.
Device Settings:-		
<i>Device Pool</i>	The device pool of the current device.	This field cannot be updated via this page.
<i>Gateway Voice Interface</i>	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is a mandatory field.	This is a mandatory field but cannot be updated via this page.
<i>Common Device Configuration</i>	Specify the common device configuration	-
<i>Call Classification</i>	Used to specify if calls are classified as <i>onnet</i> or <i>offnet</i> . Select the required value from the drop-down list.	This is a mandatory field. If you would prefer to use the system default, select the <i>use system default</i> option.
<i>Media Resource Group List</i>	Select the required Media Resource Group List from the drop-down list.	Media Resource Group Lists cannot be added here, please ensure the required list has been configured before attempting to configure a gateway.
<i>Location</i>	The current location related to the device.	This is a mandatory field but cannot be updated via this page.
<i>Packet Capture Mode</i>	Used to specify the packet capture mode. Options include <i>Batch Processing mode</i> and <i>None</i> . Select the required value from the drop-down list.	This is a mandatory field.
<i>Packet Capture Duration</i>	Specify the required packet capture duration.	-
<i>Media Termination Point Required</i>	Select this checkbox if the gateway requires a media termination point.	Determines whether or not a Media Termination Point (MTP) is used to implement features that H.323 does not support (such as hold and transfer).
<i>Retry Video Call as Audio</i>	Select this checkbox if you would like the system to redial video calls as an audio call.	-

Field	Description	Notes
<i>Unattended Port</i>	Select this checkbox if this is going to be an unattended port.	-
<i>sRTP Allowed</i>	Select this checkbox if you would like to enable the use of sRTP for this gateway.	-
<i>Trusted Relay Point</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>On</i> and <i>Off</i> .	-
Call Routing Information:-		
<i>Remote-Party-Id</i>	Select this checkbox if you would like to utilize <i>Remote-Party-Id</i>	-
<i>Asserted-Identity</i>	Select this checkbox if you would like to enable <i>Asserted-Identity</i> .	-
<i>Asserted-Type</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>PAI</i> and <i>PPI</i> .	This is a mandatory field.
<i>SIP Privacy</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>ID</i> and <i>ID Critical</i> .	This is a mandatory field.
<i>MLPP Domain ID</i>	Select the required value from the drop-down list.	-
Call Routing Information - Inbound Calls:-		
<i>Significant Digits</i>	Use the drop-down list to specify the significant digits for this gateway, alternately, select the <i>All</i> option.	This is a mandatory field. Significant digits are counted from the right (last digit) of the number called.
<i>Connected Line ID Presentation</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
<i>Connected Name Presentation</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
<i>Calling Search Space</i>	Select the required calling search space from the drop-down list	-
<i>AAR Calling Search Space</i>	Select the required AAR calling search space from the drop-down list.	Automated alternate routing (AAR) handles the calls that are routed to the AAR Destination Mask or Voice Mail.
<i>Prefix DN</i>	This is used to specify the prefix digits that are appended to the called party number on incoming calls. Specify the required Prefix DN using the provided text field	-
<i>Redirecting Diversion Header Delivery - Inbound</i>	Select this checkbox if Redirecting Diversion Header Delivery - Inbound	-
Call Routing Information - Outbound Calls:-		

Field	Description	Notes
<i>Calling Party Selection</i>	Any outbound call on a gateway can send directory number information. Use the drop-down list to specify which number is sent.	This is a mandatory field.
<i>Calling Line ID Presentation</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
<i>Calling Name Presentation</i>	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
<i>Caller ID DN</i>	Enter the pattern that you would like to use for calling line ID	Field accepts 0 to 24 digits.
<i>Caller Name</i>	Specify the required value in the provided text field.	-
<i>Redirecting Diversion Header Delivery - Outbound</i>	Select this checkbox if Redirecting Diversion Header Delivery - Outbound	
SIP Information:-		
<i>Destination Address</i>	The destination address of the gateway.	This is a mandatory field but cannot be modified via this page.
<i>Destination Address is an SRV</i>	Select this checkbox if the destination address is an SRV	
<i>Destination Port</i>	Specify the required port of the gateway.	This is a mandatory field.
<i>MTP Preferred Originating Codec</i>	The MTP Preferred Originating Codec for the gateway.	This field cannot be modified via this page.
<i>Presence Group</i>	Specify the presence group for the gateway.	This is a mandatory field.
<i>SIP Trunk Security Profile</i>	Specify the SIP Trunk Security Profile.	This is a mandatory field.
<i>Rerouting Calling Search Space</i>	Select the required value from the drop-down list.	-
<i>Out-Of-Dialog Refer Calling Search Space</i>	Select the required value from the drop-down list.	-
<i>SUBSCRIBE Calling Search Space</i>	Select the required value from the drop-down list.	-
<i>SIP Profile</i>	Specify the required SIP profile.	This is a mandatory field.
<i>DTMF Signalling Method</i>	Select the required value from the drop-down list.	This is a mandatory field.

H.323 Gateway Configuration

H.323 gateways are configured in the system via the *H.323 Gateway Configuration* page.

Procedure

Follow these steps to configure a H.323 Gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Complete all of the required fields and click the **Submit** button.

The gateway will be configured.

The following fields are available when configuring a H.323 Gateway:

Field	Description	Notes
Device Information:-		
<i>Name</i>	Name of the device currently being modified.	This field cannot be updated via this page.
<i>Protocol</i>	Protocol of the device currently being modified.	This field cannot be updated via this page.
<i>IP Address</i>	This is the IP address used to configure the Gateway itself and could be different to the IP address defined on the IOS device screen (often it is the same).	This field cannot be updated via this page.
<i>IP Address (alternate)</i>	Alternate IP Address of the device currently being modified.	This field cannot be updated via this page.
<i>IP Address B</i>	This is the IP address that other devices, for example Unified CMs, use when communicating with the Gateway.	This field cannot be updated via this page.
Device Settings:-		
<i>Call Classification</i>	Used to specify if calls are classified as <i>onnet</i> or <i>offnet</i> . Select the required value from the drop-down list.	This is a mandatory field. If you would prefer to use the system default, select the <i>use system default</i> option.
<i>Packet Capture Mode</i>	Used to specify the packet capture mode. Options include <i>Batch Processing mode</i> and <i>None</i> . Select the required value from the drop-down list.	This is a mandatory field
<i>Gateway Voice Interface</i>	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is a mandatory field.	This is a mandatory field
<i>Tunneled Protocol</i>	Used to select the required tunnel protocol. Select the required value from the drop-down list.	This is a mandatory field
<i>Signaling Port</i>	Enter the required signaling port into the text field.	This is a mandatory field

Field	Description	Notes
<i>Media Resource Group List</i>	Select the required Media Resource Group List from the drop-down list.	Media Resource Group List s cannot be added here, please ensure the required list has been configured before attempting to configure a gateway.
<i>MLPP Domain ID</i>	Enter the MLPP domain ID	-
<i>Retry Video Call as Audio</i>	Select this check-box if you would like the system to redial video calls as an audio call.	-
<i>Packet Capture Duration</i>	Specify the required packet capture duration.	-
<i>sRTP Allowed</i>	Select this check-box if you would like to enable the use of sRTP for this gateway.	-
<i>Wait for Far End H.245 Terminal Capability Set</i>	Select this check-box if you would like the gateway to wait to establish the far end terminals capabilities.	-
<i>Media Termination Point Required</i>	Select this check-box if the gateway requires a media termination point.	Determines whether or not a Media Termination Point (MTP) is used to implement features that H.323 does not support (such as hold and transfer).
Call Routing Information - Inbound Calls:-		
<i>Significant Digits</i>	Use the drop-down list to specify the significant digits for this gateway, alternately, select the <i>All</i> option.	This is a mandatory field. Significant digits are counted from the right (last digit) of the number called.
<i>Calling Search Space</i>	Select the required calling search space from the drop-down list	-
<i>AAR Calling Search Space</i>	Select the required AAR calling search space from the drop-down list	Automated alternate routing (AAR) handles the calls that are routed to the AAR Destination Mask or Voice Mail.
<i>Prefix DN</i>	Specifies the prefix digits that are appended to the called party number on incoming calls. Specify the required Prefix DN using the provided text field.	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls
<i>Redirecting Number IE Delivery - Inbound</i>	Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.	Redirecting Number IE is for voice-messaging integration only. Note: The default setting is to leaves this check-box unchecked.
<i>Enable Inbound FastStart</i>	Check this check box to enable the FastStart call connections.	Note: For inter cluster calls, the <i>Enable Inbound FastStart</i> check-box must be selected for all clusters.
Call Routing Information - Outbound Calls:-		

Field	Description	Notes
<i>Calling Party Selection</i>	Any outbound call on a gateway can send directory number information. Use the drop-down list to specify which number is sent.	This is a mandatory field
<i>Calling Party Presentation</i>	Use the drop-down list to specify whether the calling party phone number is displayed or restricted.	-
<i>Called party IE number type unknown</i>	Use the drop-down list to select the format for the number type in called party directory numbers.	This is a mandatory field
<i>Calling party IE number type unknown</i>	Use the drop-down list to select the format for the number type in called party directory numbers.	This is a mandatory field
<i>Called Numbering Plan</i>	Use the drop-down list to select the format for the numbering plan in called party directory numbers.	This is a mandatory field
<i>Calling Numbering Plan</i>	Use the drop-down list to select the format for the numbering plan in calling party directory numbers.	This is a mandatory field
<i>Caller ID DN</i>	Enter the pattern that you would like to use for calling line ID	Field accepts 0 to 24 digits.
<i>Display IE Delivery</i>	Select this check-box to enable delivery of the display IE in SETUP, CONNECT, and NOTIFY messages for the calling and called party name delivery service.	-
<i>Redirecting Number IE Delivery - Outbound</i>	Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Call Manager.	The Redirecting Number IE is for voice-messaging integration only. Note: Default leaves the check box unchecked.
<i>Enable Outbound FastStart Codec</i>	Select this check box to enable the H.323 FastStart feature on outgoing calls.	-
<i>Codec For Outbound FastStart</i>	Using the drop-down list provided, select the codec for use with the H.323 device for an outbound FastStart call.	-

Field	Description	Notes
<i>Calling Party Transformation CSS</i>	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	Select the required value from the drop-down list. Note: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> check box (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
<i>Use device pool calling party transformation CSS</i>	-	Checkbox selected=Feature enabled. Checkbox not selected=feature disabled.
<i>Called Party Transformation CSS</i>	Select the Called Party Transformation CSS that contains the called party transformation patterns that should be applied to calls routed through the trunk.	This is a mandatory field. Select the required value from the drop-down list. You can also leave this set to <i>None</i> and use the Called Party Transformation CSS assigned to the device pool by selecting the <i>Use device pool called party transformation CSS</i> check box (see below).
<i>Use device pool called party transformation CSS</i>	-	Checkbox selected=Feature enabled. Checkbox not selected=feature disabled.

Gateway Hardware Configuration

Procedure

Add a new Gateway Hardware Configuration

Follow these steps to add a new Gateway Hardware Configuration:

- Step 1** Browse to *Network > IOS Devices*
- Step 2** Select the **Active link (Host Name)** of the IOS device that you would like to add a Gateway Hardware Configuration profile to
- Step 3** Select the required **Gateway** (active text link) then select the **Gateway Hardware Configuration** button
- Step 4** Select Gateway Chassis and then select the **Next** button
- Step 5** Select **Modules** and then select the **Next** button
- Step 6** Select the **Voice Interface Cards** for each Module then complete the required fields
- Step 7** Select the **Save** button to finalize the gateway configuration

Note

Depending on the configuration of your system, available fields may differ.

Available fields include:

Field	Description	
<i>Host Name</i>	The Host Name of the IOS device.	
<i>Connected Device Type</i>	Specifies the device the IOS Gateway is connecting to	
<i>Protocol</i>	The protocol for the gateway. This is a mandatory field.	
<i>MAC Address</i>	This is the MAC address of the gateway. This must be 12 characters and is a mandatory field.	
<i>Gateway Chassis</i>	Select the required Gateway Chassis from the drop-down list. This is a mandatory field. Select the Modify button to modify the Gateway Chassis.	
<i>Module Slot</i>	Select the contents of the Module Slot from the drop-down list. Once you have made a selection, further drop-down lists will appear for the relevant cards, such as Voice Interface cards. Select the relevant cards from the drop-down lists.	
<i>Gateway Voice Interface</i>	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is a mandatory field.	
<i>ISDN Switch Type</i>	Select the required switch type from the drop-down list.	
<i>Switchback Timing</i>	Select the required timing from the drop-down list. The options include Delayed, Graceful, Immediate and Scheduled.	
<i>Switchback uptime-delay</i>	The uptime delay specified in minutes. The default is ten (10) minutes.	
<i>Switchback Schedule</i>	Specify the switchback schedule time. The time is specified in the format hh:mm.	
<i>Type of DTMF Relay</i>	Select the required DTMF Relay from the drop-down list. The options include, Current GW Config, NSE, NTE-CA, NTE-GW, and Out of Band.	

Field	Description	
<i>Supplementary Services</i>	Select to enable Supplementary Services, including voicemail, call forwarding, conferencing and speed dials to be managed at location level as analog line features. Only available for SCCP analog gateways.	

Procedure

Modifying a Gateway

Follow these steps to modify a Gateway:

- Step 1** Browse to *Network > IOS Devices*
- Step 2** Select the **Active link (Host Name)** of the IOS device that you would like to modify a Gateway for
- Step 3** Select the **Active link** (name) of the Gateway that you would like to modify
- Step 4** Select the Gateway Chassis then select the **Next** button
- Step 5** Select the **Modules** and select the **Next** button
- Step 6** Select the **Voice Interface Cards** for each Module and complete the required fields
- Step 7** Select the **Save** button to finalize the gateway configuration

The Gateway will be updated within the system.

Procedure

Modifying a Gateway Chassis

Follow these steps to modify a Gateway Chassis:

- Step 1** Browse to *Network > IOS Devices*
- Step 2** Select the **Active link (Host Name)** of the IOS device that has the Gateway you would like to modify
- Step 3** Select the **Active link** (name) of the Gateway that you would like to modify
- Step 4** Select the Modify button adjacent to the Gateway Chassis that you would like to modify
- Step 5** Select the **Save** button to finalize the Gateway Chassis configuration

The Gateway will be updated within the system.

IOS Gateway Wizards

To assist users with the addition of IOS Gateways in the system, a number of predefined workflows, called wizards, are provided. These wizards include predefined workflows defined to assist and guide users through the setup and configuration of common gateway workflows. The benefits of using the wizards include:

- The wizards combine the various steps (add IOS device, add gateway, configure gateway, add ports, etc.) into a single workflow that can be completed in one transaction. The user does not

need to complete the entire workflow, they can choose to stop the workflow and apply the changes as and when required. Once completed, all the transactions will be initiated based on how far the workflow was completed.

- The wizard preselects certain configuration parameters to make the workflow easier and to guide the user based on the type of gateway they are adding.

These options appear when adding an IOS device and are the recommended way of adding the IOS devices as some options are preselected to make the workflow smoother. Once the gateway is added through the wizard, it can be modified and managed like a normal gateway. If a wizard isn't available for the type of gateway needed, the custom IOS device option can be used to go through the individual steps with all options available.

Procedure

To add an IOS Gateway using a wizard:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the required wizard. Options include:
- IPPBX Connect
 - MGCP VG2xx Analog Gateway
 - IPPBX Connect SCCP VG2xx Analog Gateway
 - IPPBX Connect SIP VG2xx Analog Gateway
 - Transit Connected MGCP Legacy PBX Gateway
 - IPPBX Connected MGCP Local Gateway
 - IPPBX Connected H.323 Local Gateway
- Step 4** Complete all of the required fields and proceed through all of the pages or up until a point where you would like to exit the wizard.

Note

See the table under "Adding a SIP Gateway Screen" in the *IOS Gateway Feature Guide* for information about the available fields.

Modifying a Gateway Role

Procedure

To modify a Gateway role:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Device*.
- Step 3** Select the *Gateway* in the *Gateway Details* section within the *Device Role* section.

Note

Gateway functions may not be unchecked when ports have been allocated.

- Step 4** Click the **Modify** button to save changes to the Gateway Details and Gateway Functions.

Interface Details

Available Interfaces are all ports that have been configured and have not yet been allocated.

Gateway Hardware Configuration

If no configuration exists for the selected gateway, you will be required to add the gateway hardware configuration. If the gateway is configured, you will be taken to the maintenance page.

Note

The *tunneledProtocol* parameter used for the addition and modification of H323 Gateways is not supported in 6.1 and 5.1 *Unified CM* versions. Users of these particular Unified CM versions must set the *tunneledProtocol* on the Unified CM itself.

To add a new Gateway Hardware configuration:

Note

Location device pools [excluding System (EMCC) and SRST types] available at the Location are displayed via a drop-down list on the configuration page of various port types such as POTS, Ground Start, Loop Start, Digital PRI, Digital T1, etc. Select or modify the Device Pool by selecting from the *Device Pool* drop-down list on the relevant screen, for example MGCP FXS POTS Port.

Scenario 1: MGCP & SCCP Gateways connected to an IPPBX

Procedure

- Step 1** Click the **Gateway Hardware Configuration** button on the Gateway form.
- Step 2** Select the Gateway Chassis from the list then click the **Next** button.
- Step 3** Select the *Modules* from the list then click the **Next** button.
- Step 4** Select the *Voice Interface Cards* for each Module and the required details, then click the **Save** button.

Note

In this scenario, the ports for the gateway will be automatically added when the Gateway Hardware Configuration is saved. The ports are created based on the voice interface card selected.

Scenario 2: H323 Gateway connected to an IPPBX

Procedure

- Step 1** Click the **Gateway Hardware Configuration** button on the *Gateway* page.
- Step 2** Fill in the required gateway details then click the **Submit** button.

Note

In this scenario, the ports for the gateway are manually added after the Gateway Hardware Configuration has been saved.

Scenario 3: SIP Gateway connected to an IPPBX

Procedure

- Step 1** Click the **Gateway Hardware Configuration** button on the *Gateway* form.
- Step 2** Complete the required gateway details then click the **Submit** button.
-

Scenario 4: MGCP Gateway connected to a Transit Switch

Procedure

- Step 1** Click the **Gateway Hardware Configuration** button on the *Gateway* form.
- Step 2** Select *Legacy Protocol* from the list then click the **Next** button.
- Step 3** Complete the required gateway details then click the **Add** button.
-

Note

In this scenario, the ports for the gateway are manually added after the Gateway Hardware Configuration has been saved.

Maintain Gateway Hardware Configuration

Green colored port buttons indicate configured and red colored ports indicate unconfigured ports. To configure a port, or to change the configuration, select the respective port button.

To change the configuration, click the **Change Device Setup** button.

To delete the configuration, click the **Delete** button.

Gateway Hardware Configuration: Ports

Ports are configured using the *Gateway Hardware Configuration* screen. From this screen you are able to:

Note

Once a port has been activated at a location it cannot be reconfigured. Such ports must first be deactivated at the location before they can be reconfigured.

- Configure unconfigured ports
- Modify configured ports
- Delete configured ports
- Change device Setup
- Delete the device

Procedure

Accessing the Gateway Hardware Configuration page

To access the *Gateway Hardware Configuration* screen:

-
- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name of the Gateway* (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Click the **Config Port Range** button.

The resultant *Gateway Hardware Configuration* screen displays the following information:

- Host Name
- Gateway Name
- Connected Device Type
- Protocol SCCP
- MAC Address
- Gateway Chassis
- Gateway Voice Interface
- ISDN Switch Type 5E9
- Switchback Timing Immediate
- Switchback uptime-delay (min)
- Switchback Schedule (hh:mm)
- Type of DTMF
- Fax mode
- Modem Passthrough

- Step 6** To complete the required tasks:
- **Configure unconfigured ports:** To configure unconfigured ports, select the checkboxes next to the relevant unconfigured ports, then click the **Configure** button.
 - **Modify configured ports:** To modify configured ports, select the checkboxes next to the relevant configured ports, then click the **Modify** button.
 - **Delete configured ports:** To delete configured ports, select the checkboxes next to the relevant configured ports, then click the **Delete** button.
 - **Change device setup:** To change the device setup, click the **Change Device Setup** button.
 - **Delete the device:** To delete the device, select the **Delete** button.

Note

- The *Select all* and *Unselect all* active text links can be used to select/deselect all ports within a section.
 - Due to a limitation of AXL provisioning, port allocation on two or more VWIC cards on the AIM-VOICE-30-SLOT-0 mainboard is not supported. This board is only available on the 3725 and 3745 chassis for MGCP gateways, and is the only choice for slot 0 on the 3725 and 3745 chassis.
-

IOS Device Port Configuration

Gateways connected to Cisco Unified Communications Manager (Unified CM)

After the Gateway Hardware configuration has been completed and saved, when you click the **Gateway Hardware Configuration** button, a list of all the ports for the gateway will be displayed.

Configured and unconfigured ports are displayed separately; the ports are further grouped by port type.

To configure an individual port, click on the link showing the port number. For unconfigured ports, complete the form fields and click **Add**. For configured ports, click **Modify** to update the details, or **Delete** to delete the configuration.

To configure a range of ports, select the checkboxes adjacent to the ports to be deleted, configured or modified then select the **Configure Selected**, **Modify Selected** or **Delete Selected** button as appropriate. The **Select All** or **Unselect All** links will select or de-select all the checkboxes in a group. Only like ports, those with the same port type and protocol, can be selected in this manner.

Once the port range has been selected, the **Configure Selected** button will lead to a page that lists all of the required fields for the selected port type. Select the checkboxes adjacent to the fields that you would like to modify and click the **Next** button. The next page will display the port range vertically, one line per port, and the selected fields horizontally, spreadsheet-style. Complete the required fields for each port then click the **Add** or **Modify** buttons to save the configuration details for each port.

Note

When modifying ports that have already been configured, all configuration is done on one page. Select the checkboxes adjacent to the fields that you would like to modify then specify the required fields.

At this stage, the information is stored and no device configuration is completed. The configuration of the IOS device, the PGW and or the IPPBX is completed once the port is allocated and assigned to its respective Gateway Function. In the case of an Analog port, the configuration of the device is completed when the port is configured at the location.

Gateways connected to LegacyPBX or Transit Switch

Unlike the gateways connected to the Unified CM, after the Gateway Hardware Configuration has been completed, the hardware components (chassis, modules and voice interface cards) within the gateway are not known. Therefore, before any ports can be configured, the ports need to be manually added to the gateway.

Procedure

To add a port to the gateway:

- Step 1** Click the **Gateway Hardware Configuration** button.
 - Step 2** At the bottom of the *Gateway Hardware Configuration* page, click the **Add Port** button.
 - Step 3** Enter the *Port Type*, the *Port Number* and the *Port Description*; then click the **Add** button.
-

On the *Gateway Hardware Configuration* page, you can verify that the port has been added to the system.

Configured and unconfigured ports are displayed separately, and ports are further grouped by port type.

To configure an individual port, select the *port number* (active text link). For unconfigured ports, complete the fields then click the **Add** button. For configured ports, click the **Modify** button to update the details or the **Delete** button to delete the configuration.

To configure a range of ports, select the checkboxes next to the ports that you would like to modify, configure or delete, and then click the **Configure Selected**, **Modify Selected** or **Delete Selected** button as appropriate. The **Select All** link will select or de-select all the checkboxes in a group.

Only like ports, those with the same port type and protocol, can be selected in this manner. For configured ports, **Delete** will cause the configuration to be deleted. For unconfigured ports, **Delete Selected Ports** will remove the selected ports from the gateway.

Once the port range has been selected, the **Configure Selected** button will lead to a page that lists all of the required fields for the selected port type.

Select the checkboxes adjacent to the fields that you would like to modify and click the **Next** button. The next page will display the port range vertically, one line per port, and the selected fields horizontally, spreadsheet-style. Complete the required fields for each port then click the **Add** or **Modify** buttons to save the configuration details for each port.

Note

When modifying ports that have already been configured, all configuration is done on one page. Select the checkboxes adjacent to the fields that you would like to modify then specify the required fields.

Like the MGCP/SCCP gateways connected to a Unified CM, the information is stored and no device configuration is completed. The configuration of the IOS device, the PGW and/or the IPPBX is completed once the port is allocated and assigned to its respective Gateway Function. In the case of an Analog port, the configuration of the device is completed when the port is configured at the location.

To modify the port settings, select the *Manage* link to the right of the port to display the required port configuration page.

Supported Port Types

Protocol	Connect Device Type	Port Type					
		E1	T1	BRI	E&M	FXO	FXS
MGCP	IPPBX	Y	Y	Y		Y	Y
	Transit Switch	Y	Y				
SCCP	IPPBX			Y			Y
H.323	IPPBX	Y	Y	Y	Y	Y	Y
SIP	IPPBX						Y

Configuring the Various Port Types

Ports are configured on various screens as shown in the examples below:

SIP Port Configuration

SIP ports are configured in the system via the Configure *SIP Port* page.

Procedure

Modify a SIP Port

To configure a SIP Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant port (active text link).
- Step 6** Complete all of the required fields and click the **Submit** or **Add** button.

The port is configured within the system.

Important

Depending on the configuration of your system, not all of the fields mentioned below will be available in your system.

The following fields are available when configuring a SIP Port:

Field	Description	Notes
Port Details:-		
Port Number	The number of the port being configured	This field cannot be updated via this page and is displayed for information purposes only.
Port Type	The type of port being configured	This field cannot be updated via this page and is displayed for information purposes only.
Port Description	Enter an optional description for the port being configured	
Port Configuration:-		
Signal	Select the required signal type from the drop-down list. Options include <i>loop-start</i> and <i>ground-start</i>	
Call Progress Tone	Select the required country from the drop-down list.	
Ring Frequency	Use the drop-down list to specify the required ring frequency for the selected Foreign Exchange Station (FXS) voice port.	
Ring Pattern	Select the required preset ring pattern from the drop-down list.	

Procedure**Modify a Range of SIP Ports**

Follow these steps to modify a range of SIP ports:

- Step 1** Browse to *Network > IOS Devices*.

-
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Select the **Gateway Hardware Configuration** button.
- Step 5** Select the **checkboxes** adjacent to the ports that you would like to modify.
- Step 6** Click the **Modify Selected** button
- Note:** If you have selected unconfigured ports, click the **Configure Selected** button.
- Step 7** Select the **checkboxes** adjacent to the fields that you would like to modify, and then click the **Next** button.
- Note**
- When modifying ports that have already been configured, all configuration is done on the first page. Select the checkboxes adjacent to the fields that you would like to modify, complete the required fields, and then click the **Modify** button.
- Step 8** Modify all of the required fields then click the **Submit** or **Add** button.

The ports are updated within the system.

Procedure

Delete a SIP Port

To delete a SIP Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant port (active text link).
- Step 6** Click the **Delete** button.

The port is deleted from the system.

SCCP Gateway FXS SCCP Port

FXS SCCP ports are managed in the system via the *SCCP Gateway FXS SCCP Port* page.

Procedure

Modifying a configured FXS port

To modify a configured FXS port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.

Step 4 Click the **Gateway Hardware Configuration** button.

Step 5 Click the **Configure Port Range** button.

Step 6 Select the **Port Name** (active text link) from the *FXS Configured* section.

Note: To edit multiple FXS SCCP ports, select the checkboxes adjacent to the required ports and then click the **Modify Selected** button.

Step 7 Complete the required fields then click the **Modify** button. The port is updated.

The following fields are available:

Field	Description	Notes
Phone Type:-		
Product Type	The type of product, for example, analog phone.	This field is for information purposes only and cannot be modified via this page.
Device Protocol	The protocol of the device, for example, SCCP.	This field is for information purposes only and cannot be modified via this page.
Device Information:-		
Mac Address	The device name of the device.	This field is for information purposes only and cannot be modified via this page.
Description	A description for the device.	This is an optional field.
Phone Button Template	Select the required phone button template from the drop-down list.	This is a mandatory field.
Apply Configuration to all Unconfigured FXS Ports	Select this checkbox if you would like to apply this Configuration to all Unconfigured FXS ports.	-
Location Specific Settings:-		
Calling Search Space	The calling search space for the location.	This field is for information purposes only and cannot be modified via this page.
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Location	The location that the device is related to.	This field is for information purposes only and cannot be modified via this page.
Network Locale	The locale for the location.	This field is for information purposes only and cannot be modified via this page.
Call Progress Tone	Select the relevant country from the drop-down list.	-
Ring Frequency	Specify the ring frequency using the drop-down list.	25 or 50
Signal	Specify the signal type using the drop-down list.	Loop-start or ground-start.

Field	Description	Notes
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.	Select the required value from the drop-down list. Note: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> check box (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Use device pool calling party transformation CSS	Select this checkbox to use the selected device pool's calling party transformation CSS.	Checkbox selected=Feature enabled. Checkbox not selected=feature disabled.

Procedure

Delete a Configured FXS Port

To delete a configured FXS port:

- Step 1** Browse to the FXS port configuration page using the steps above.
- Step 2** Click the **Delete** button.

After confirming the operation, the port is deleted.

Note: To delete multiple FXS SCCP ports, select the checkbox adjacent to the required ports and then click the **Delete Selected** button.

Procedure

Modifying Multiple FXS Ports

- Step 1** Browse to the *Port Range Configuration* page using the steps above.
- Step 2** Select the checkboxes adjacent to the required ports then click the **Modify Selected** button.
- Step 3** Select the required fields then click the **Next** button.

Note

When modifying ports that have already been configured, all configuration is done on the first page. Select the checkboxes adjacent to the fields that you would like to modify, complete the required fields then click the **Modify** button.

The following page lists all of the selected ports and enables you to modify on a per-port basis. Available fields include:

- Description
- Phone button Template

- Call Progress
- Tone
- Ring Frequency
- Signal

Step 4 Modify the required fields then click the **Modify** button.

The selected fields are updated.

SCCP BRI Port

SCCP BRI ports are managed in the system via the *SCCP BRI Port* page.

Procedure

Configuring a BRI Port

To modify a BRI Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant **Port Name** (active text link), for example *0(BRI)*.
- Step 6** Complete the required fields then click the **Add** button.

The port is configured.

The following fields are available:

Field	Description	Notes
Device Information:-		
IP Address	IP Address of the device.	This field is for information purposes only and cannot be modified via this page.
Device Name	MAC address of the device.	This field is for information purposes only and cannot be modified via this page.
Description	A short description of the device being modified.	This is a mandatory field.
Device Pool	The Device Pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Phone Button Template	Select the required phone button template from the drop-down list.	-
Location	The location that the device is associated with.	This field is for information purposes only and cannot be modified via this page.

Field	Description	Notes
Network Locale	The network Locale of the device, for example, United Kingdom.	This field is for information purposes only and cannot be modified via this page.
Always use Prime Line	Specifies whether the device will always use the prime line. Select the required option from the drop-down list. The options include <i>on</i> and <i>off</i> .	This is a mandatory field.
Always use Prime Line for Voice Message	Specifies whether the device will always use the prime line for voice messages. Select the required option from the drop-down list. The options include <i>on</i> and <i>off</i> .	This is a mandatory field.
ISDN Switch Type	Select the ISDN switch type from the drop down list.	-
Ignore Presentation Indicators (internal calls only)	Select this checkbox if you would like the device to ignore the presentation indicators.	Select this checkbox to configure call display restrictions on a call-by-call basis. When selected, Unified CM ignores any presentation restrictions that are received for internal calls.
Allow Control of Device from CTI	Select this checkbox to allow CTI to control and monitor this device.	-
Logged into Hunt Group	Select this checkbox if you would like the device to automatically log into hunt groups.	Note Users can log in and out of hunt groups using their phones soft-keys.
Remote Device	Select this checkbox if the device is a remote device.	Use this option if you are experiencing delayed connect times over SCCP pipes to remote sites. Enabling this checkbox tells Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone.

MGCP FXS POTS Port Configuration

MGCP FXS POTS ports are configured in the system via the *MGCP FXS POTS Port* page.

Procedure

To configure a MGCP FXS POTS Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.

- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0 (FXS)** or **1 (FXS)** button as applicable.
- Step 7** Select the *POTS* Port Name (active text link).
- Step 8** Complete all of the required fields and click the **Add** button. The gateway port is configured.

The following fields are available when configuring a MGCP FXS POTS Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Description of the gateway currently being modified.	This field cannot be updated via this page.
Device Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	Select the checkbox (if required) to edit the description field.
Location Specific Settings		
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Location	The current location related to the device.	This field cannot be updated via this page.
Network Locale	The current network locale within the Location.	This field cannot be updated via this page.
Transmit UTF-8 for Calling Party Name	<p>This device uses the user locale setting of the SIP trunks to determine whether to send Unicode and whether to translate received Unicode information.</p> <p>For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII.</p> <p>The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters</p>	<p>Select or deselect the checkbox as required.</p> <p>Note</p> <p>The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.</p>

Field	Description	Notes
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	<p>Select the required option from the drop-down list.</p> <p>Note</p> <p>Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> checkbox (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</p>
Use device pool calling party transformation CSS	Select this checkbox to use the selected device pool's calling party transformation CSS.	Checkbox selected=feature enabled, checkbox not selected=feature disabled.
POTS Port Information:-		
Port Direction	The port direction, namely <i>Inbound</i> , <i>Outbound</i> , or <i>Bothways</i> .	This is a mandatory field. Select the required port direction from the drop-down list.
Prefix DN	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls.	The system adds prefix digits after first truncating the number in accordance with the Num Digits setting.
Num Digits	Enter the number of significant digits to collect, from 0 to 32.	<p>This is a mandatory field. Enter the required number of digits.</p> <p>The system counts significant digits from the right (last digit) of the number called.</p> <p>Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that is used to route calls coming into the PRI span. See also <i>Prefix DN</i> above.</p>
Expected Digits (0-32)	Enter the number of digits that are expected on the inbound side of the trunk.	<p>This is a mandatory field. Enter the required number of digits (0 to 32).</p> <p>Leave zero as the default value if you are unsure.</p>

Field	Description	Notes
SMDI Port Number (0-4096)	This field is used for analog access ports that connect to a voice-mail system.	This is a mandatory field. Enter the required port number. Set the SMDI Port Number equal to the actual port number on the voicemail system to which the analog access port connects. Note Voicemail logical ports typically must match physical ports for the voicemail system to operate correctly.
Unattended Port	Select this checkbox if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this checkbox is unchecked.	Select the checkbox if this is an unattended port.
Call Progress Tone	The country of the call progress tone.	Select the from the drop-down list.
Ring Frequency	Ring frequency is usually country dependent, and you should take into account the appropriate ring frequency for your area before you configure this field.	Select the required ring frequency (25 or 50 from the drop-down list.
Ring Pattern	Ring pattern is usually country dependent, and you should take into account the appropriate ring pattern for your area before you configure this field. See also <i>Ring Frequency</i> above.	Select the required ring pattern (<i>pattern01</i> to <i>pattern12</i> from the drop-down list.

MGCP FXS Loop Start Port Configuration

MGCP FXS Loop Start ports are configured in the system via the *MGCP FXS Loop Start Port* page.

Procedure

To configure a MGCP FXS Loop Start Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.
- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0 (FXS)** or **1 (FXS)** button as applicable.
- Step 7** Select the *Loop Start Port Name* (active text link).
- Step 8** Complete all of the required fields and click the **Add** button. The gateway port is configured.

The following fields are available when configuring a MGCP FXS Loop Start Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Description of the gateway currently being modified.	This field cannot be updated via this page.
Device Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	This field cannot be updated via this page.
Location Specific Settings		
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Location	The current location related to the device.	This field cannot be updated via this page.
Network Locale	The current network locale within the Location.	This field cannot be updated via this page.
Transmit UTF-8 for Calling Party Name	<p>This device uses the user locale setting of the SIP trunks to determine whether to send Unicode and whether to translate received Unicode information.</p> <p>For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII.</p> <p>The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters.</p>	<p>Select or deselect the checkbox as required.</p> <p>Note: The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.</p>

Field	Description	Notes
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	Select the required option from the drop-down list. Note: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> check box (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Use device pool calling party transformation CSS	Select this checkbox to use the selected device pool's calling party transformation CSS.	Checkbox selected=feature enabled, checkbox not selected=feature disabled.
Port Information (Loop Start)		
<i>Port Direction</i>	The selected port direction, namely <i>Inbound</i> , <i>Outbound</i> , or <i>Bothways</i> .	This is a mandatory field. Select the required port direction from the drop-down list.
Attendant DN	The number to which you want incoming calls routed.	This is a mandatory field. Enter the number to which you want incoming calls routed, for example zero or a directory number for an attendant.
Unattended Port	Check this checkbox if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this check box is unchecked	Select the checkbox if this is an unattended port.
Call Progress Tone	The call progress tone for your country.	Select the from the drop-down list.
Ring Frequency	Ring frequency is usually country dependent, and you should take into account the appropriate ring frequency for your area before you configure this field.	Select the required ring frequency (25 or 50 from the drop-down list.
Ring Pattern	Ring pattern is usually country dependent, and you should take into account the appropriate ring pattern for your area before you configure this field. See also Ring Frequency above.	Select the required ring pattern (<i>pattern01</i> to <i>pattern12</i>) from the drop-down list.

MGCP FXS Ground Start Port Configuration

MGCP FXS Ground Start ports are configured in the system via the *MGCP FXS Ground Start Port* page.

Procedure

To configure a MGCP FXS Ground Start Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.
- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0 (FXS)** or **1 (FXS)** button as applicable.
- Step 7** Select the *Ground Start Port Name* (active text link).
- Step 8** Complete all of the required fields and click the **Add** button. The gateway port is configured.

The following fields are available when configuring a MGCP FXS Ground Start Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Description of the gateway currently being modified.	This field cannot be updated via this page.
Device Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	This field cannot be updated via this page.
Location Specific Settings		
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Location	The current location related to the device.	This field cannot be updated via this page.
Network Locale	The current network locale within the Location.	This field cannot be updated via this page.

Field	Description	Notes
Transmit UTF-8 for Calling Party Name	<p>This device uses the user locale setting of the SIP trunks to determine whether to send Unicode and whether to translate received Unicode information.</p> <p>For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII.</p> <p>The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters.</p>	<p>Select or deselect the checkbox as required.</p> <p>Note: The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.</p>
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	<p>Select the required option from the drop-down list.</p> <p>Note: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> check box (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</p>
Use device pool calling party transformation CSS	Select this checkbox to use the selected device pool's calling party transformation CSS.	Checkbox selected=feature enabled, checkbox not selected=feature disabled.
Port Information (Ground Start)		
<i>Port Direction</i>	Choose the direction of calls that pass through this port: The selected port direction, namely <i>Inbound</i> , <i>Outbound</i> , or <i>Bothways</i> .	<p>This is a mandatory field. Select the required port direction from the drop-down list.</p> <p><i>Inbound</i>. Use for incoming calls only.</p> <p><i>Outbound</i>. Use for outgoing calls.</p> <p><i>Bothways</i>. Use for incoming and outgoing calls.</p>

Field	Description	Notes
Attendant DN	The number to which you want incoming calls routed.	This is a mandatory field. Enter the number to which you want incoming calls routed, for example zero or a directory number for an attendant.
Unattended Port	Check this checkbox if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this check box is unchecked	Check the checkbox if this is an unattended port.
Call Progress Tone	The call progress tone for your country.	Select the from the drop-down list.
Ring Frequency	Ring frequency is usually country dependent, and you should take into account the appropriate ring frequency for your area before you configure this field.	Select the required ring frequency (25 or 50 from the drop-down list.
Ring Pattern	Ring pattern is usually country dependent, and you should take into account the appropriate ring pattern for your area before you configure this field. See also <i>Ring Frequency</i> above.	Select the required ring pattern (<i>pattern01</i> to <i>pattern12</i> from the drop-down list.

MGCP FXO Port

Procedure

MGCP FXO Port Configuration

MGCP FXO ports are configured in the system via the *MGCP FXO Port* page.

To configure a MGCP FXO Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.
- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0 (FXO)** or **1 (FXO)** button as applicable.
- Step 7** Complete all of the required fields and click the **Add** button. The FXO port is configured.

The following fields are available when configuring a MGCP FXO Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Description of the gateway currently being modified.	This field cannot be updated via this page.

Field	Description	Notes
Device Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	This field cannot be updated via this page.
Location Specific Settings:-		
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Location	The current location related to the device.	This field cannot be updated via this page.
Network Locale	The current network locale within the Location.	This field cannot be updated via this page.
Transmit UTF-8 for Calling Party Name	<p>This device uses the user locale setting of the SIP trunks to determine whether to send Unicode and whether to translate received Unicode information.</p> <p>For the sending device, if you check this check box and the user locale setting in the device's device pool matches the terminating phone's user locale, the device sends Unicode. If the user locale settings do not match, the device sends ASCII.</p> <p>The receiving device translates incoming Unicode characters based on the user locale setting of the sending device's device pool. If the user locale setting matches the terminating phone's user locale, the phone displays the characters.</p>	<p>Select or deselect the checkbox as required.</p> <p>Note: The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.</p>
Called Party Transformation CSS	Select the Called Party Transformation CSS that contains the called party transformation patterns that should be applied to calls routed through the trunk.	<p>This is a mandatory field. Select the required option from the drop-down list.</p> <p>You can also leave this set to <i>None</i> and use the Called Party Transformation CSS assigned to the device pool by selecting the <i>Use device pool called party transformation CSS</i> check box (see below).</p>
Use device pool called party transformation CSS	Select this checkbox to use the selected device pool's called party transformation CSS.	Checkbox selected=feature enabled, checkbox not selected=feature disabled.
Port Information:-		

Field	Description	Notes
<i>Signal</i>	The selected signal, namely <i>Ground Start</i> , or <i>Loop Start</i> .	This is a mandatory field. Select the required signal from the drop-down list.
<i>Port Direction</i>	The selected port direction, namely <i>Inbound</i> , <i>Outbound</i> , or <i>Bothways</i> .	This is a mandatory field. Select the required port direction from the drop-down list.
Attendant DN	The specified Attendant DN.	This is a mandatory field. Specify the required Attendant DN using the provided text field.
Unattended Port	Select this checkbox if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port. The default value for this checkbox is unchecked	Select the checkbox if this is an unattended port.
Call Progress Tone	The country of the call progress tone.	Select the from the drop-down list.
Dial Type	The selected dial type, namely <i>MF</i> , <i>DTMF</i> , or <i>Pulse</i> .	Select the required dial type from the drop-down list.
Ring Number	The selected ring number.	Select the required ring number (<i>Default</i> to <i>10</i>) from the drop-down list.

H.323 Port Configuration

H.323 ports are configured in the system via the Configure *H.323 Port* page.

Procedure

Modify a H.323 Port

To configure a H.323 Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant port (active text link).
- Step 6** Complete all of the required fields and click the **Modify** button.

The port is configured within the system.

Important

Depending on the configuration of your system, not all of the fields mentioned below will be available in your system.

The following fields are available when configuring a H.323 Port:

Field	Description	Notes
Port Details:-		

Field	Description	Notes
Port Number	The number of the port being configured	This field cannot be updated via this page and is displayed for information purposes only.
Port Type	The type of port being configured	This field cannot be updated via this page and is displayed for information purposes only.
Port Description	Enter an optional description for the port being configured	
Port Configuration:-		
Framing	Select the required framing method from the drop-down list. Available options include <i>ESF</i> and <i>SF</i> .	
Clock Source	Select the required value from the drop-down list. Available options include <i>internal</i> and <i>line</i>	
Line Coding	Select the required line Coding type from the drop-down list.	
Pri-Group Timeslots	Specify the pri-group timeslots using the provided text field	
Interface Serial	Specify the interface serial using the provided text field	
ISDN Switch Type	Select the required ISDN Switch type from the drop-down list.	Available options include: <ul style="list-style-type: none"> • primary-net5 • primary-4ess • primary-5ess • primary-dms100 • primary-net5 • primary-in • primary-ntt • primary-qsig
ISDN Bchannel Number Order	Select whether you would like the ISDN Bchannel order to be <i>ascending</i> or <i>descending</i> . This is specified using the provided drop-down list.	
Set Called Party Number NOA for Outgoing calls	Select this checkbox if you would like to set the called party number NOA for outgoing calls	Default setting is No. This field can only be modified if the trunk hasn't been activated in a location
Set Calling Party Number NOA for Outgoing calls	Select this checkbox if you would like to set the calling party number NOA for outgoing calls	Default setting is No. This field can only be modified if the trunk hasn't been activated in a location

Field	Description	Notes
Local Dialing Method	Select the required Local Dialing Method from the drop-down list.	Available options include: <ul style="list-style-type: none"> • No Local Dialing • 10-digit dialing • Local Dialing without Area Code
National Area Code (for local dialing)	Specify the national area code that will be used for local dialing	This is a numeric field with a max length of 10. This is an optional setting and the default is empty. This field can only be modified if the trunk hasn't been activated in a location
Non-ISR two tuple port	This checkbox should be used when a Non-ISR router is used where the controller interface number is 2 tuple (eg 0/0) but the voice port numbering is 3 tuple (eg 0/0/0).	This option enables the system to generate the correct voice port number for IOS configuration. The default value is for it not to be selected

Procedure

Delete a H.323 port

To delete a H.323 Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant port (active text link)
- Step 6** Click the **Delete** button. The port is deleted from the system.

Port Configuration

Ports are configured in the system via the *Configure Port* page.

Procedure

Modify a Port

Follow these steps to configure a port:

- Step 1** Browse to *Network > IOS Devices*
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.

- Step 5** Select the relevant port (active text link).
- Step 6** Complete all of the required fields and click the **Submit** or **Add** button.

The port is configured within the system.

Important

Depending on the configuration of your system, not all of the fields mentioned below will be available in your system.

The following fields are available when configuring a Port:

Field	Description	Notes
Port Details:-		
Port Number	The number of the port being configured.	This field cannot be updated via this page and is displayed for information purposes only.
Port Type	The type of port being configured.	This field cannot be updated via this page and is displayed for information purposes only.
Port Description	Enter an optional description for the port being configured.	
Port Configuration:-		
Signal	Select the required signal type from the drop-down list. Options include <i>loop-start</i> and <i>ground-start</i> .	-
Call Progress Tone	Select the required call progress tone from the drop-down list.	-
Ring Frequency	Use the drop-down list to specify the required ring frequency for the selected Foreign Exchange Station (FXS) voice port.	-
Ring Pattern	Select the required preset ring pattern from the drop-down list.	-

Procedure

Modify a Range of Ports

To modify a range of ports:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the *checkboxes* adjacent to the ports that you would like to modify.
- Step 6** Click the **Modify Selected** button.

Note

If you have selected unconfigured ports, click the **Configure Selected** button.

- Step 7** Select the *checkboxes* adjacent to the fields that you would like to modify, then click the **Next** button.

Note

When modifying ports that have already been configured, all configuration is done on the first page. Select the checkboxes adjacent to the fields that you would like to modify, complete the required fields then click the **Modify** button.

- Step 8** Modify all of the required fields then click the **Submit** or **Add** button.

The ports are updated within the system.

Procedure**Delete a Port**

To delete a Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the **Host Name** (active text link) that you would like to modify.
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Select the relevant port (active text link).
- Step 6** Click the **Delete** button. The port is deleted from the system.
-

Digital T1 Port Configuration

Digital T1 ports are configured in the system via the *Digital T1 Port Configuration* page.

Procedure

To configure a Digital T1 Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.
- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0(T1)** button.
- Step 7** Select the *Digital T1 Port Name* (active text link).

Step 8 Complete all of the required fields and click the **Add** button. The gateway port will be configured.

The following fields are available when configuring a T1 Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Name of the gateway currently being modified.	This field cannot be updated via this page.
Device Protocol	Name of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	-
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Call Classification	Available options are: <i>Not Selected</i> , <i>OFFNET</i> , <i>ONNET</i> or <i>Use System Default</i>	This is a mandatory field. Select the required option from the drop-down list.
Port Selection Order	Specifies the order in which ports are enabled from first (lowest number port) to last (highest number port), or from last to first	This is a mandatory field. Select the required option from the drop-down list. <i>Top Down</i> (last to first) or <i>Bottom Up</i> (first to last). Note: If you are not sure which port order to use, select the <i>Top Down</i> option.
Digit Sending	Select the required method to send digits, available options are: <i>Not Selected</i> , <i>DTMF</i> , <i>MF</i> , or <i>Pulse</i>	This is a mandatory field. Select the required option from the drop-down list.
Called Party Transformation CSS	Select the Called Party Transformation CSS that contains the called party transformation patterns that should be applied to calls routed through the trunk.	This is a mandatory field. Select the required option from the drop-down list. You can also leave this set to <i>None</i> and use the Called Party Transformation CSS assigned to the device pool by selecting the <i>Use device pool called party transformation CSS</i> check box (see below).
Use device pool called party transformation CSS	Select this checkbox to use the selected device pool's called party transformation CSS.	Checkbox selected=feature enabled, checkbox not selected=feature disabled.
Product Specific Configuration Layout:-		

Field	Description	Notes
Line Coding	Determines how the T1 span electrically codes binary 1's and 0's on the wire (line coding selection).	<p>This is a mandatory field. Select the required line coding option from the drop-down list.</p> <p><i>AMI</i> Alternate Mark Inveesion</p> <p><i>B8ZS</i> (Bipolar 8-Zeros Substitution)</p> <p><i>HDB3</i> (High-density Bipolar 3)</p> <p>AMI is used on older T1 circuits and references signal transitions with a binary 1, or "mark." B8ZS, a more reliable method, is more popular and is recommended for PRI configurations as well. B8ZS encodes a sequence of eight zeros in a unique binary sequence to detect line-coding violations. HDB3 is a form of zero-suppression line coding.</p>
Framing	Ensure the framing format configured on the port matches the framing format of the line.	<p>This is a mandatory field. Select from the drop-down list.</p> <p>Digital T1 lines use the SF or ESF framing format. SF provides two-state, continuous supervision signaling, in which a 0 bit value is used to represent on-hook and a 1 bit value is used to represent off-hook. ESF robs four bits instead of two, yet has little impact on voice quality. ESF is required for 64-kbps operation on DS0 and is recommended for Primary Rate Interface (PRI) configurations.</p>
Clock	Specifies the clock with which to synchronize. External (from the line) or internal to the router's digital interface.	<p>This is a mandatory field. Select from the drop-down list.</p> <p>If the timing source is internal, timing derives from the onboard phase-lock loop (PLL) chip in the digital voice interface. If the timing source is line (external), timing derives from the PBX or PSTN CO to which the voice port is connected. It is generally preferable to derive timing from the PSTN because PSTN clocks are maintained at an extremely accurate level. This is the default setting for the clock source.</p>
Pri-Group Timeslots	-	This field cannot be updated via this page.
Interface Serial	-	This field cannot be updated via this page.

Field	Description	Notes
ISDN Switch Type	-	Select from the drop-down list. Contact your service provider for the correct values to use if required.
Input Gain (-6..14 db)	-	This is a mandatory field. Enter the required value.
Output Attenuation (-6..14 db)	-	This is a mandatory field. Enter the required value.
Echo Cancellation Enable	-	This is a mandatory field. Select from the drop-down list.
Echo Cancellation Coverage (ms)	-	This is a mandatory field. Select from the drop-down list.

Digital PRI or MGCP/SCCP E1 Port Configuration

Digital PRI or E1 ports are configured in the system via the *Digital PRI Port Configuration* or *MGCP/SCCP E1 Port Configuration* page respectively.

Procedure

To configure a Digital PRI or MGCP/SCCP E1 Port:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the required *Provider Name* (active text link).
- Step 3** Select the *Host Name* of the Gateway (active text link) that you would like to modify.
- Step 4** Select the required Gateway Details *Name* (active text link) that you would like to modify.
- Step 5** Click the **Gateway Hardware Configuration** button.
- Step 6** Click the **0 (T1)** button to configure a PRI Port or the **0 (E1)** button to configure an MGCP/SCCP E1 Port.
- Step 7** Select the *Digital PRI Port Name* (active text link) if you pressed the **0 (T1)** button.
- Step 8** Complete all of the required fields and click the **Add** button. The gateway port will be configured.

The following fields are available when configuring a PRI Port or MGCP/SCCP E1 Port:

Field	Description	Notes
Device Information:-		
Product	Name of the port currently being modified.	This field cannot be updated via this page.
Gateway	Description of the gateway currently being modified.	This field cannot be updated via this page.
Device Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
End-Point Name	Name of the port currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	This field cannot be updated via this page.

Field	Description	Notes
Device Pool	The device pool to which the port is assigned.	Select the required device pool from the drop-down list, which displays all device pools available to the location, excluding EMCC type system and SRST.
Call Classification	Available options are: <i>OFFNET</i> , <i>ONNET</i> or <i>Use System Default</i>	This is a mandatory field. Select the required option from the drop-down list.
Interface Information:-		
PRI Protocol Type	The communications protocol for the span.	This is a mandatory field. Select the required option from the drop-down list. Note: This should be determined by the switch to which you are connecting as well as the preferred protocol.
Protocol Side	Displays the port protocol emulation. <i>Network</i> = port configured as a master, <i>User</i> = port configured as a slave.	This is a mandatory field. Select the required option from the drop-down list.
Channel Selection Order	Specifies the order in which ports are enabled from first (lowest number port) to last (highest number port), or from last to first.	This is a mandatory field. Select the required option from the drop-down list. <i>Top Down</i> (last to first) or <i>Bottom Up</i> (first to last). Note: If you are not sure which port order to use, select the <i>Top Down</i> option.
Channel IE Type	Indicates whether channel selection is presented as a channel map or a slot map.	This is a mandatory field. Select the required option from the drop-down list. <i>Number</i> = channel usage always channel map format, <i>Slotmap</i> = channel usage always slotmap format or <i>Use Number when 1B</i> = channel usage is channel map for one B-channel but slotmap if more than one B-channel.
PCM Type	Specifies the digital encoding format.	This is a mandatory field. Select the required option from the drop-down list. <i>A-law</i> = Europe and Rest of the World, <i>uLaw</i> = North America and Japan.

Field	Description	Notes
Delay for first restart (1/8 sec ticks)	Controls the rate at which the spans are brought in service when Inhibit Restarts at PRI Initialization is disabled.	This is a mandatory field. Enter the required value (default=32). Use this option when many PRI spans are enabled on a system and Inhibit Restarts at PRI Initialization is disabled.
Delay between restarts (1/8 sec ticks)	Determines the length of time between restarts if Inhibit Restarts is disabled, when a PRI RESTART is sent.	This is a mandatory field. Enter the required value (default=4).
Call Routing Information - Inbound Calls:-		
Significant Digits	Specifies the number of significant digits to collect, from <i>0 to 32</i> or <i>All</i> .	This is a mandatory field. Select the relevant option from the drop-down list. If you select <i>All</i> , the inbound number is not truncated. For example, the digits received are 123456. The Significant Digits setting is 4. Digits translated are 3456. Use to process incoming calls, and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that come into the PRI span. See also <i>Prefix DN</i> below.
Prefix DN	Specifies the prefix digits that are appended to the called party number on incoming calls. Specify the required Prefix DN using the provided text field.	Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls.
Call Routing Information - Outbound Calls:-		
Calling Party Presentation	Specifies whether to transmit or block the caller's phone number. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field. Select the required option from the drop-down list.

Field	Description	Notes
Calling Party Selection	Specifies which DN is sent. Any outbound call on a gateway can send directory number information.	<p>This is a mandatory field. Use the drop-down list to specify which number is sent.</p> <p><i>Originator</i> = send the calling device's DN.</p> <p><i>First Direct Number</i> = send DN of the redirecting device.</p> <p><i>First Redirect Number (External)</i> = send DN of first redirecting device with external phone mask applied.</p> <p><i>Last Redirect Number</i> = send DN of the last device to redirect the call.</p> <p><i>Last Redirect Number (External)</i> = send DN of the last redirecting device with the external phone mask applied.</p>
Called Party IE number type unknown	Available options include <i>Cisco Call Manager, International, National, Subscriber</i> or <i>Unknown</i> .	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>Note: We recommend that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. Contact support for more information if required.</p>
Calling Party IE number type unknown	Available options include <i>Cisco Call Manager, International, National, Subscriber</i> or <i>Unknown</i> .	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>Note: We recommend that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. Contact support for more information if required.</p>
Called Numbering Plan	Available options include <i>Cisco Call Manager, ISDN, National Standard, Private</i> or <i>Unknown</i> .	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>Note: We recommend that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. Contact support for more information if required.</p>

Field	Description	Notes
Calling Numbering Plan	Available options include <i>Cisco Call Manager</i> , <i>ISDN</i> , <i>National Standard</i> , <i>Private</i> or <i>Unknown</i> .	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>Note: We recommend that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. Contact support for more information if required.</p>
Number of digits to strip	The number of digits to strip on outbound calls, from 0 to 32.	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>For example, when 8889725551234 is dialed, and the number of digits to strip is 3, the system strips 888 from the outbound number.</p>
Caller ID DN	The pattern that you would like to use for calling line ID.	Enter the required digits 0 to 24.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	<p>Select the required value from the drop-down list.</p> <p>Note: Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you check the <i>Use device pool calling party transformation CSS</i> check box (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</p>
Use device pool calling party transformation CSS	Select this checkbox to use the selected device pool's calling party transformation CSS.	Checkbox selected=Feature enabled. Checkbox not selected=feature disabled.
Called Party Transformation CSS	Select the Called Party Transformation CSS that contains the called party transformation patterns that should be applied to calls routed through the trunk.	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>You can also leave this set to <i>None</i> and use the Called Party Transformation CSS assigned to the device pool by selecting the <i>Use device pool called party transformation CSS</i> check box (see below).</p>

Field	Description	Notes
Use device pool called party transformation CSS	Select this checkbox to use the selected device pool's called party transformation CSS.	Checkbox selected=Feature enabled. Checkbox not selected=feature disabled.
PRI Protocol Type Specific Information:-		
Display IE Delivery	Check the checkbox to enable delivery of the display information element (IE) in SETUP, and NOTIFY messages (for DMS protocol) for the calling and connected party name delivery service.	Default = unchecked
Redirecting Number IE Delivery - Outbound	<p>Check this checkbox to include the Redirecting Number IE in the outgoing SETUP message from the system to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.</p> <p>Uncheck the checkbox to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message.</p> <p>You use the Redirecting Number IE for voice-mail integration only. If your configured voice-mail system supports Redirecting Number IE, you should check the checkbox.</p>	Default = unchecked
Redirecting Number IE Delivery - Inbound	<p>Check this checkbox to accept the Redirecting Number IE in the incoming SETUP message to the system.</p> <p>Uncheck the checkbox to exclude the Redirecting Number IE in the incoming SETUP message to the system.</p> <p>You use Redirecting Number IE for voice-mail integration only. If your configured voice-mail system supports Redirecting Number IE, you should check the checkbox.</p>	Default = unchecked
Send Extra Leading Character in Display IE	<p>Check this checkbox to include a special leading character byte (non ASCII, nondisplayable) in the Display IE field.</p> <p>Uncheck this checkbox to exclude this character byte from the DisplayIE field. This checkbox only applies to the DMS-100 protocol and the DMS-250 protocol.</p>	Default = unchecked

Field	Description	Notes
Setup non-ISDN Progress Indicator IE Enable	<p>Enable this setting only if users do not receive ringback tones on out-bound calls. When this setting is enabled, the system sends Q.931 SETUP messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN.</p> <p>This message notifies the destination device that the gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with systems that connect to PBXs through digital gateways.</p>	Default = unchecked
MCDN Channel Number Extension Bit Set to Zero	To set the channel number extension bit to zero, check the checkbox. To set the extension bit to 1, uncheck the check box.	<p>Set checkbox as required.</p> <p>This setting only applies to the DMS-100 protocol.</p>
Send Calling Name in Facility IE	<p>Check the checkbox to send the calling name in the Facility IE field. Set this feature for a private network that has a PRI interface enabled for ISDN calling name delivery.</p> <p>When this checkbox is checked, the calling party's name gets sent in the Facility IE of the SETUP or FACILITY message, so the name can display on the called party's device.</p>	<p>Default = unchecked</p> <p>Set this feature for PRI trunks in a private network only. Do not set this feature for PRI trunks connected to the PSTN.</p>
Interface Identifier Present	Check the checkbox to indicate that an interface identifier is present.	<p>Default = unchecked</p> <p>This setting only applies to the DMS-100 protocol for digital access gateways in the Channel Identification information element (IE) of the SETUP, CALL PROCEEDING, ALERTING, and CONNECT messages.</p>
Interface Identifier Value	This field applies to only the DMS-100 protocol.	<p>Enter the value that was obtained from the PBX provider.</p> <p>Valid values range from 0 to 255.</p>
Connected Line ID Presentation (QSIG In-bound Call)	Whether the system allows or blocks the connected party's phone number from displaying on an in-bound caller's phone. Available options are: <i>Default</i> , <i>Allowed</i> or <i>Restricted</i> .	This is a mandatory field. Select the required option from the drop-down list.
UUIE Configuration:-		

Field	Description	Notes
Passing Precedence Level Through UUIE	-	Select the checkbox to enable the feature if required.
Security Access Level	The desired security access level.	This is a mandatory field. Enter the required security access level.
Product Specific Configuration Layout:-		
Line Coding	Determines how the T1 span electrically codes binary 1's and 0's on the wire (line coding selection).	This is a mandatory field. Select the required line coding option from the drop-down list. <i>AMI</i> (Alternate Mark Inversion) <i>B8ZS</i> (Bipolar 8-Zeros Substitution)
Framing	The framing value. Available framing options are: <i>CRC4</i> , <i>D4</i> , <i>ESF</i> , <i>Non CRC4</i> or <i>SF</i> .	This is a mandatory field. Select the required framing option from the drop-down list.
Clock	Either from the system (Internal) or the Provider (External)	This is a mandatory field. Select the required clock option from the drop-down list. Default=External
PRI Group Timeslots	Used to configure Non-Facility Associated Signaling (NFAS) and specify the channels to be controlled by the primary NFAS D channel. Contact your supplier for more details if required.	Enter the required value.
Interface Serial	-	Enter the required value.
ISDN Switch Type	-	Select from the drop-down list.
Input Gain (-6..14db)	The input gain.	This is a mandatory field. Enter the required input gain (-6db minimum to 14db maximum).
Output Attenuation (-6..14db)	The output attenuation.	This is a mandatory field. Enter the required output attenuation (-6db minimum to 14db maximum).
Echo Cancellation Enable	-	This is a mandatory field. Select <i>Enable</i> or <i>Disable</i> from the drop-down list.
Echo Cancellation Coverage (ms)	Available options (in ms) are: <i>24</i> , <i>32</i> , <i>48</i> or <i>64</i> .	Select the required value from the drop-down list.

Service Details

This section is only visible if ports have been configured. Each enabled gateway function provides a configuration section.

PSTN Interfaces

This feature is available when PSTN is selected at *Gateway Functions*.

PSTN ports may be allocated to any location or customer of the provider depending on the port allocation setting. Click the **Port Allocation** button to allocate PSTN ports.

Analog Interfaces

This function is available when the *Analog* feature is activated. Analog ports may only be allocated to locations within the selected port allocation level.

Click the **Port Allocation** button to allocate analog ports.

Legacy Interfaces

Identical to PSTN interfaces.

Delete a Gateway Role

Procedure

To delete a gateway role:

- Step 1** Browse to *Network > IOS Device*.
- Step 2** Select the *Device Name*.
- Step 3** Select the *Gateway* in the *Gateway Details* section within *Device Roles*.
- Step 4** Click the **Delete** button to remove the IOS Gateway.

Note

A gateway may only be deleted if no IPPBX is connected to it.

Media Resources Role

Adding a Hardware Media Resource

Procedure

Note

Existing profiles on the IOS device may cause configuration conflicts when adding a hardware media resource.

To add a media resource:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the Host *Name* (active text link) of the IOS device that you would like to add a hardware media resource to.
- Step 3** Click the **Add** button adjacent to the hardware media resource device role that you would like to configure.
- Step 4** Complete the required fields (see table below for field details).

Field	Description	Remarks
Name	The name of the media resource.	This is a mandatory field.
Select Device	Select an IPPBX from the drop-down list.	This is a mandatory field.

Field	Description	Remarks
NAT of Connected Device Address to Gateway	This setting determines which address (real or NAT) is used when configuring the gateway with the call agent addresses. If selected, the NAT address is used. If not selected, the real address is used. The checkbox, by default, is not selected. Note: The NAT of Connected Device Address to Gateway option is only for Unified CMs. An error message is returned if a Unified CM is not being used and/or NAT is not configured for the Unified CM. Transit switches cannot be used with this setting.	Select checkbox if required.
Gateway Voice Interface	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets.	This is a mandatory field.

Step 5 Select Hardware Media Resources (HMR) to configure, that is the required media resource types. The available types are:

- Conferencing
- Transcoding
- MTP (Media Termination Point)

Step 6 Click the **Add** button when complete.

Procedure

Modifying Hardware Media Resources

To modify hardware media resources:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) of the IOS device that you would like to modify.
- Step 3** Select the *Name* (active text link) of the hardware media resource that you would like to modify.
- Step 4** Modify the values as required then click the **Modify** button. The changes to hardware media resource details and gateway functions are saved.

Procedure

Deleting Hardware Media Resources

To delete hardware media resources:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) of the IOS device that you would like to delete a hardware media resource from.
- Step 3** Select the *Name* (active text link) of the hardware media resource that you would like to delete.
- Step 4** Click the **Delete** button. The hardware media resource is removed from the IOS device.
-

Configuring Hardware Media Resources**Procedure**

To configure Hardware Media Resources:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) of the IOS device that you would like to modify.
- Step 3** Select the *Configure* link of the Hardware Media Resource that you would like to configure. The *Manage IOS Hardware Resources* screen is displayed.
- Step 4** Click the **Add** button associated with the Hardware Media Resource type for which configuration details are to be provided (see below).
- Transcoding : see [Transcoding Configuration on page 260](#)
 - Conferencing : see [Conferencing Configuration on page 261](#)
 - MTP : see [MTP Configuration on page 262](#)
- Step 5** Provide the values as required then click the **Add** button.
-

Transcoding Configuration**Procedure**

To add transcoder configuration details:

- Step 1** Click the **Add** button in the *Transcoding Details* section on the *Manage IOS Hardware Media Resources* screen. The *IOS Device - Add Transcoder* screen is displayed.
- Step 2** Complete the required information in the *Transcoder Details* section (see table below for details).

Field	Description
Name	The name of the transcoder role. This is a mandatory field. Note <ul style="list-style-type: none">• Names across multiple HMR roles must be unique per Unified CM. No duplicate names allowed.• Enter up to 15 characters. Minimum of 6 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).
Description	A description of the transcoder role.

Field	Description
Transcoder Type	Select an available transcoder type from the list. This is a mandatory field.
Device Pool	Select the required device pool from the drop-down list. The transcoder hardware media resource type inherits certain properties from this device pool, for example location and region.
Slot	The slot on the chassis of the router where the voice interface will be connected. Valid values are e.g. 0, 0/0, 0/0/0.IOS. This is a mandatory field.
Codecs	<p>The codecs of the IOS device. Provide the exact name of the codecs. Valid codecs are g711alaw, g711ulaw, g722-64, g729abr8, g729ar8, g729br8, g729r8, ilbc.</p> <p>Multiple codecs are supported using a ' ; ' as the delimiter.</p> <p>Note</p> <ul style="list-style-type: none"> • Duplicate codecs entered into any of the codecs boxes are deleted before an attempt at provisioning is made. • The default codec block is always built in IOS config when adding a hardware media resource, irrespective of your codec type input. • If a subset of the default codecs is specified in the CUCDM, the entire default codec block is still built. • If only non-default codecs are added via CUCDM, these are added in addition to the default codecs.
Max Sessions	Number of session supported by the profile. Range is 0 to X, default is 0. The X value is determined at run time depending on the number of resources available with the resource provider. This is a mandatory field.

Conferencing Configuration

Procedure

To add conferencing configuration details:

- Step 1** Click the **Add** button in the *Conferencing Details* section on the *Manage IOS Hardware Media Resources* screen. The *IOS Device - Add Conferencing* screen is displayed.
- Step 2** Complete the required information in the *Conference Details* section (see table below for details).

Field	Description
Name	<p>The name of the conference role. This is a mandatory field.</p> <p>Note</p> <ul style="list-style-type: none"> • Names across multiple HMR roles must be unique per Unified CM. No duplicate names allowed. • Enter up to 15 characters. Minimum of 6 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).
Description	A description of the conference role.

Field	Description
Conference Type	Select an available conference type from the list. This is a mandatory field.
Device Pool	Select the required device pool from the drop-down list. The conferencing hardware media resource type inherits certain properties from this device pool, for example location and date/time group.
Slot	The slot on the chassis of the router where the voice interface will be connected. Valid values are 0, 0/0, 0/0/0.IOS. This is a mandatory field.
Codecs	<p>The codecs of the IOS device. Provide the exact name of the codecs. Valid codecs are g711alaw, g711ulaw, g722-64, g729abr8, g729ar8, g729br8, g729r8, ilbc.</p> <p>Multiple codecs are supported using a ' ; ' as the delimiter.</p> <p>Note</p> <ul style="list-style-type: none"> • Duplicate codecs entered into any of the codecs boxes are deleted before an attempt at provisioning is made. • The default codec block is always built in IOS config when adding a hardware media resource, irrespective of your codec type input. • If a subset of the default codecs is specified in the CUCDM, the entire default codec block is still built. • If only non-default codecs are added via CUCDM, these are added in addition to the default codecs.
Max Sessions	Number of session supported by the profile. Range is 0 to X, default is 0. The X value is determined at run time depending on the number of resources available with the resource provider. This is a mandatory field.

Step 3 Click the **Add** button when complete.

MTP Configuration

Procedure

To add MTP configuration details:

Step 1 Click the **Add** button in the *MTP Details* section on the *Manage IOS Hardware Media Resources* screen. The *IOS Device - Add MTP* screen is displayed.

Step 2 Complete the required information in the *MTP Details* section (see table below for details).

Field	Description
Name	<p>The name of the MTP role. This is a mandatory field.</p> <p>Note</p> <ul style="list-style-type: none"> • Names across multiple HMR roles must be unique per Unified CM. No duplicate names allowed. • Enter up to 15 characters. Minimum of 6 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).

Field	Description
Description	A description of the MTP role.
Device Pool	Select the required device pool from the drop-down list. The MTP hardware media resource type inherits certain properties from this device pool, for example location and region.
Slot	The slot on the chassis of the router where the voice interface will be connected. This is a mandatory field. Valid values are 0, 0/0, 0/0/0.IOS.
Codecs	<p>The codecs of the IOS device. Provide the exact name of the codecs. Valid codecs are g711alaw, g711ulaw, g722-64, g729abr8, g729ar8, g729br8, g729r8, ilbc.</p> <p>Multiple codecs are supported using a ';' as the delimiter.</p> <p>Note</p> <ul style="list-style-type: none"> • Duplicate codecs entered into any of the codecs boxes are deleted before an attempt at provisioning is made. • The default codec block is always built in IOS config when adding a hardware media resource, irrespective of your codec type input. • If a subset of the default codecs is specified in the CUCDM, the entire default codec block is still built. • If only non-default codecs are added via CUCDM, these are added in addition to the default codecs.
Max Sessions	Number of session supported by the profile. Range is 0 to X, default is 0. The X value is determined at run time depending on the number of resources available with the resource provider. This is a mandatory field.

Step 3 Click the **Add** button when complete.

Deleting a Hardware Media Resource

Procedure

To delete a Hardware Media Resource:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the Host *Name* (active text link) of the IOS device that you would like to delete a Hardware Media Resource from.
- Step 3** Select the *Name* (active text link) of the Hardware Media Resource that you would like to delete.
- Step 4** Click the **Delete** button to remove the Hardware Media Resource. The Hardware Media Resource will be removed from the system.

SRST Role

For an overview of the SRST functionality and role, see [The Survivable Remote Site Telephony \(SRST\) on page 355](#).

To assign the SRST role to an IOS Device, refer to [SRST Role on page 355](#).

Media Service Management

Media services include Conference, Music on Hold, Presence and other media related services.

Note

For Media Services to be offered at the Location level, the services must be created at the Provider level and allocated to the Customers' Locations.

Procedure

Adding a Media Service**Note**

Before media services are added, make sure that the relevant Media Servers have been added to the system.

To add a Media Service:

- Step 1** Browse to *Resources > Media Services*.
- Step 2** Click the **Add** button.
- Step 3** Complete the relevant fields and click the **Add** button.

The Media Service is added to the system.

The following fields are available:

Field	Description
Name *	Enter a name for the Media Service, this is a mandatory field.
Description	Enter a short description for the media service you are adding
Select Media Resource Group List Name	Select the relevant media resource group list name from the drop-down list.

Procedure

Delete a Media Service

To delete a Media Service:

- Step 1** Browse to *Resources > Media Services*.
- Step 2** Select the Media Service that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the delete operation, the Media Service is deleted from the system.

Configure Per-Port COS for Emergency Calls from Analog Ports

Analog ports on H.323 and SIP Gateways do not support per-port Call Search Space (CSS) 'natively', as other ports do.

This feature adds the ability to configure per-port COS for analog ports on H323 and SIP gateways.

When the gateway is activated, the user has the ability to activate per-port COS for analog ports on H323 and SIP gateways.

Activate Per-Line COS for Analog Gateways

Pre-requisites:

- A SIP or H323 analog gateway must be registered on the system.
- The Analog gateway function must be enabled for the gateway.
- An FXS port(s) must exist on the gateway.

For more information on adding and modifying gateways and ports, see under [IOS Device Management on page 205](#).

Procedure

To activate Per-Port COS for Analog gateways:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the Host *Name* (active text link) of the relevant SIP or H323 device.
- Step 3** In the Gateway Details section, click on the *Name* (active text link) of the gateway on which Per-Port COS is to be enabled.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** In the Inbound Calls section, select the *Enable Per-Port COS* checkbox.

Note

- When *Per-Port COS* is enabled the 'Per-port COS on analog gateway' option is pre-selected in the *Calling Search Space* field. The user cannot select any other option from the drop-down list.
- The 'Per-port COS on analog gateway' selection creates an analog gateway COS to apply to the ports on the gateway.
- Enabling *Per-Port COS* on the gateway allows *Per-Port COS* (and the analog gateway COS) to be activated on individual ports.

- Step 6** Click the **Modify** button.

The administrator can now activate *Per-Port COS* for a port on the gateway, by registering the port.

Activate Per-Port COS for Analog Ports

Procedure

To activate Per-Port COS for analog ports:

- Step 1** Browse to *Location Administration > Analog Line Mgt*.
- Step 2** Click on the relevant Gateway *Name* (active text link).

- Step 3** In the Available Ports section, click the **Register** button associated with the port for which you want to register a line.
- Step 4** Select the relevant Feature Group from the drop-down list.
- Step 5** Click the **Next** button.
- Step 6** Provide all the required details of the line.
- Step 7** The *Line Class of Service* drop-down list is now displayed.
- Step 8** Click the **Register** button. The analog gateway COS is applied to the port.

The same process can be followed to update a registered analog port. (click the **Unregister** button to deregister the port.)

For more information on registering, as well as updating an analog port, see [Analog Port Management on page 268](#).

Supplementary Services on Analog Gateways

Supplementary Services, including voicemail, call forwarding, conferencing and speed dials can be enabled on a SCCP VG2xx Analog Gateway. Supplementary Services can then be managed at location level as analog line features. The availability of supplementary services depends on whether the service is enabled in the relevant Feature Group, as well as whether the service is supported by SCCP.

Procedure

To provision Supplementary Services:

- Step 1** Enable the Supplementary Services feature for the SCCP VG2xx Analog Gateway.
- Step 2** Register an analog line on an analog port.
- Step 3** Manage the analog line's supplementary services (line features).

Enabling Supplementary Services

Procedure

To enable Supplementary Services for a new SCCP VG2xx Analog Gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button associated with SCCP VG2xx Analog Gateway.
- Step 4** Provide all the required details and click the **Next** button.
- Step 5** Select the *Supplementary Services* check-box to enable the feature.
- Step 6** Click the **Next** button.

Procedure

To enable Supplementary Services for a new Custom IOS Device:

-
- Step 1** Browse to *Network > IOS Devices*.
 - Step 2** Click the **Add** button.
 - Step 3** Click the **Custom Add** button associated with a Custom IOS Device.
 - Step 4** Complete the required information. Make sure to select the *Gateway* checkbox.
 - Step 5** Click the **Add** button.
 - Step 6** Browse to *Network > IOS Devices*.
 - Step 7** Select the relevant custom gateway *host name* (active text link) from the list.
 - Step 8** In the *Gateway Details* section, click the **Add** button next to the Gateway checkbox.
 - Step 9** Complete any outstanding information. Select 'SCCP' from the Protocol drop-down list.
 - Step 10** Click the **Next** button.
 - Step 11** Complete the required information.
 - Step 12** Click the **Next** button.
 - Step 13** Select *Analog* as the gateway type.
 - Step 14** Click the **Add** button.
 - Step 15** Browse to *Network > IOS Devices*.
 - Step 16** Select the relevant custom gateway *host name* (active text link) from the list.
 - Step 17** In the Gateway Details section, click on the *name* of the relevant gateway.
 - Step 18** Click the **Gateway Hardware Configuration** button.
 - Step 19** Complete the required information and click the **Next** button.
 - Step 20** Complete the required information and click the **Next** button.
 - Step 21** Complete the required information. Select the *Supplementary Services* checkbox to enable the feature.
 - Step 22** Click the **Save** button.
-

Procedure

To enable or disable Supplementary Services for an existing analog gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click on the relevant gateway *host name* (active text link) from the list.
- Step 3** In the *Gateway Details* section, click on the *name* of the relevant gateway.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Click the **Change Device Setup** button.
- Step 6** Click the **Next** button.
- Step 7** Click the **Next** button.
- Step 8** Enable or disable Supplementary Services by selecting or deselecting the *Supplementary Features* checkbox.

- Step 9** Click the **Update Gateway** button.

For more information on how to add, modify and delete IOS Devices, please see the IOS Device Management section in the Deployment Guide.

IOS Model Settings

When enabling Supplementary Services for a SCCP Gateway the *AddSCCP-SUPP* model is applied.

When disabling Supplementary Services for a SCCP Gateway the *DelSCCP-SUPP* model is applied.

For more information on these models, please see the IOS Model Guide.

Analog Port Management

Procedure

Register a line to a port

To register a line for an analog port:

- Step 1** Browse to *Location Administration > Analog Line Mgt.*
- Step 2** Click the *Gateway Name* (active text link) of the gateway for which you want to register a line to a port.
- Step 3** Click the **Register** button associated with the port you want to register a line for.
- Step 4** Complete the required fields in the *Details* section of the screen. The available fields include:

Field	Description
Gateway Name	The name of the gateway on which a line is being registered to the selected port.
IOS Device Name	The name of the IOS Device on which the gateway was provisioned.
Port Number	The port number of the port to which a line is being registered.
Port Type	The relevant port's type.
Description	A description for the port. The port's MAC address is used as the default value.
Feature group	Select a Feature Group from the drop-down list. Note: Select a Feature Group that only has features enabled which are supported by analog lines.

- Step 5** Click the **Next** button.
- Step 6** Complete/modify the following fields (if required) in the *Details* section of the screen:

Field	Description
Usage	Select the relevant <i>Usage</i> from the drop-down list, that is <i>Phone</i> or <i>Fax Machine</i> .
Device Pool	Select the relevant device pool from the drop-down list. The drop-down list displays all device pools available for the location.

- Step 7** Complete/modify the following fields (if required) in the *Number Details* section of the screen:

Field	Description
Number	<p>Select the line's extension number from the drop-down list.</p> <p>Note</p> <p>Although shared analog lines can be allocated across all protocols, SIP and H323 may give unexpected results due to limited support in the Unified CM.</p>
Label (ASCII - leave blank for default)	Provide a label for the line.
Line Class of Service	<p>Note</p> <ul style="list-style-type: none"> For SIP/H323, this field is only visible when the <i>Gateway Hardware Configuration</i> setting <i>Enable Per Port COS</i> checkbox is selected. When registering analog devices, the CoS you select during registration is applied to that line as well as to any other shared instances of that line. <p>Select the required line class of service to be applied to the line from the drop-down list. For SIP/H323 the drop-down list contains a list of all outbound service types associated with the current dial-plan, which have an analog COS code. For MGCP/SCCP the drop-down list contains a list of all outbound service types associated with the current dial-plan.</p>

Step 8 Click the **Register** button.

Cisco Unified Communications Domain Manager (CUCDM) registers the line to the port.

Procedure

Unregister a line from a port

To unregister a line from an analog port:

Step 1 Browse to *Location Administration > Analog Line Mgt.*

Note

From version 8.1.1, CUCDM automatically removes/clears the following dependencies (if configured) that are associated with an analog line during the unregistering an analog line process:

- Remove analog line speed dials
- A cascade delete confirmation summary popup screen is provided, which details the actions taken to automatically modify or remove related services that depend on the analogue port being registered
- Phone Busy Lamp Field references. When unregistering an analog line that is being monitored using a busy lamp field on one or more other devices, those device busy lamp fields are deleted (if the line is not shared).
- Line Groups. This analog line is removed from any associated line groups (if the line is not shared).

- Pickup Groups. This analog line is removed from any associated pickup groups (if the line is not shared).
- User Associations. If a user is associated with this analog line, they are unassociated- associated from this line. Refer to [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#) for details on these dependencies.

Step 2 Click the *Gateway Name* (active text link) of the gateway for which you want to unregister a line from a port.

Step 3 Click the **Unregister** button associated with the port you want to unregister a line for. A confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies, the analog line is immediately unregistered.

Note

The **Unregister** button is only displayed next to ports for which a line has already been registered.

Step 4 Click the **Unregister** button on the confirmation popup screen to continue with the unregister process. CUCDM removes/clears the relevant associations and unregisters the analog line from the port. Alternatively click the **Cancel** button to abort the process.

Note

The unregister transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

Analog Line Management

Procedure

Analog Line Management

To manage a registered line:

Step 1 Browse to *Location Administration > Analog Line Mgt.*

Step 2 Click on the *Gateway Name* (active text link) of the gateway for which you want to manage a line that is registered to a port.

Step 3 Click the **Line Management** button associated with the port you want to manage a line for.

Note

The Line Management button is only displayed next to ports for which a line has already been registered.

Step 4 Complete/modify the following fields (if required) in the *Port Details* area of the screen.

Field	Description
Port Number	The number for the port. This is a read-only field.
Description	A description for the port. The port's MAC address is used as the default value.

Field	Description
Line Class of Service	<p>Note</p> <ul style="list-style-type: none"> For SIP/H323, this field is only visible when the <i>Gateway Hardware Configuration</i> setting <i>Enable Per Port COS</i> checkbox is selected. When modifying analog devices, the CoS you select is applied to that line as well as to any other shared instances of that line. <p>Select the required line class of service to be applied to the line from the drop-down list. For SIP/H323 the drop-down list contains a list of all outbound service types associated with the current dial-plan, which have an analog COS code. For MGCP/SCCP the drop-down list contains a list of all outbound service types associated with the current dial-plan.</p>

Step 5 Complete the required *Private line* and *Common line* fields in the *Line Details* area of the screen.

Note

The available fields depend on the features that have been enabled in the associated Feature Group and which are available on analog lines. See under *Managing a Line* in ??? for a comprehensive list of available fields.

Step 6 Click the **Modify** button.

If there is no connectivity between the CUCDM and Unified CM, an error message is displayed, informing you that the values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the page. Click the **Sync with Call Manager** button to manually sync these values with Unified CM when connectivity has been restored.

Register an Analog Line with an Analog Port

Procedure

To register an analog line with an analog port:

Step 1 Browse to *Location Administration > Analog Line Mgt.*

Step 2 Click on the relevant *Gateway Name* (active text link).

Step 3 In the *Available Ports* section, click the **Register** button associated with the port for which you want to register a line.

Note

If a line has already been registered for the port, the **Unregister** button will display. Click this button to unregister the line from the port.

Step 4 Select the relevant *Feature Group* from the drop-down list.

Note

Select a Feature Group that only has features enabled which are available on an analog line. For more information on Feature Groups, see [Feature Group Management on page 500](#).

Step 5 Click the **Next** button.

- Step 6** Select the relevant *Usage* (i.e. 'fax' or 'phone'), the line's *Number* and *Line Class of Service* from the drop-down lists.
- Step 7** Click the **Register** button.
-

SCCP Supplementary Features

The following is a list of features that are enabled through SCCP Supplementary Features:

Note

Some of these features might overlap with native Analog Line Features.

- Audio Message Waiting Indicator
- Call forward All
- Call forward All cancel
- Call FWD on Busy
- Call Forward on No Answer
- Call Pickup Group
- Call Pickup Local
- Caller ID
- Conference Call
- Redial
- Speed Dials
- Speed Dial to voicemail
- Call Transfer
- Call Waiting
- Hook flash
- Display name (Caller Line ID)
- Line mask
- Display name ASCII

Valid Analog Line Features

The following is a list of the existing line features that are available for analog lines.

Note

These features may overlap with Supplementary Features for SCCP gateways.

- Contact Center Agent Line
- Line Class of Service
- Hold reversion ring duration
- Hold reversion notification interval
- Music on hold
- No answer ring duration
- Call forward on no coverage

- Call forward on CTI failure
- Call forward on No Coverage to voicemail
- Call forward On CTI Failure to voicemail
- Alerting Name
- Call forward - always (**Note:** This setting takes precedence over all other call forward settings, except *Call forward all calls to voicemail* - see below).
- Call forward when busy
- Call forward if no answer
- Call forward on non registered
- Call forward all calls to voicemail (**Note:** This setting takes precedence over all other call forward settings).
- Call forward calls on busy to voicemail
- Call forward on no answer to voicemail
- Call forward on non registered to voicemail
- Call forward calling search space activation policy

Key Sync Features

Key Syncing with the Cisco Unified Communications Manager (Unified CM) enabled for the following features:

- Call Forward All to voicemail
- Call Forward All

IOS Commands

IOS Devices are configured by sending sequences of commands to the device. These configuration commands are recorded for future reference. If a device is in unmanaged mode (manual mode) then the commands that would have been sent to the device are also recorded.

A number of limitations need to be considered.

Telnet Limitations

- SSH Version Limitations

IOS devices must be configured to use SSH Version 2. Issuing commands to an IOS device using SSH Version 1 results in an *Access Failed* error message. To avoid this issue, change to secure model (SSH v2) or remove the command from the model and issue it manually on the IOS device.

- Issuing Commands in Secure Mode

Due to certain limitations when interacting with the IOS device in Telnet mode, it is possible to get an error within an IOS Driver transaction similar to the example below:

```
IOSDevice 15.x : cmd[voice service VoIP ] error[command timed-out at /var/www/usm/perl/
bvsmbatch/ipt_driver_IOSDevice_15.x.pl line 1843
```

In the above example, the *voice service VoIP* command in a model caused the error. The resolution is to change to secure model (k) or to remove the command from the model and issue it manually on the IOS device. Other commands may cause a similar issue.

Procedure

Viewing Commands for an IOS Device

To view the list of commands sent to an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the appropriate device *Name* (active text link) and then click the **Command List** button.

The configuration commands that have been sent to the device are displayed. To see extra information about the commands, click the **Show Details** button. The transaction number, action type and date are displayed. This page also indicates if the IOS device was in manual mode at the time of each transaction. To remove the extra details, click the **Hide details** button.

Procedure

Viewing Commands in a Separate Window

- The list of commands may be viewed in a separate browser window. To view the list in a separate window, select the **View in new window** button.
-

Note

Some browsers that utilize pop-up window protection may not allow this action to take place, or may ask you to confirm the opening of the new window.

[Download Command List on page 284](#)

Note

Download behavior can differ amongst browsers. If you experience any difficulty while downloading command lists, consider one of the following options:

- If an error is returned when attempting to download the file, try selecting the **View in new window** button and then browse to *File > Save As* in your browser. After saving the file to a location of your choice, you can view the file as usual.
 - Alternatively, click the **Download** button and then select the *Open* option. From within the browser, browse to *File --> Save As*
-

[Exporting IOS Commands on page 284](#)

SCCP and MGCP Protocol

Procedure

SCP and MGCP Gateway Configuration

SCCP and MGCP gateways are configured in the system via the generic Gateway Hardware Configuration screen.

To configure a SCCP or MGCP gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name* (active text link) of the gateway that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.

- Step 5** Complete all of the required fields and click the **Save** button. The following fields are available when configuring a SCCP or MGCP Gateway:

Note

Depending on the configuration of your system, available fields may differ.

The gateway is configured.

Field	Description
Host Name	The Host Name of the IOS device.
Connected Device Type	Specifies the device the IOS Gateway is connecting to
Protocol	The protocol for the gateway. This is a mandatory field, that is SCCP or MGCP.
MAC Address	This is the MAC address of the gateway. This must be 12 characters and is a mandatory field.
Gateway Chassis	Select the required Gateway Chassis from the drop-down list and click Next. This is a mandatory field. Click the Modify button to modify the Gateway Chassis.
Module Slot	Select the contents of the Module Slot(s) from the drop-down list(s) and click the Next button. Once you have made a selection(s), further drop-down lists appear for the relevant cards, such as Voice Interface cards. Select the relevant cards from the drop-down lists and click the Next button.
Gateway Voice Interface	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is a mandatory field.
ISDN Switch Type	Select the required switch type from the drop-down list.
Switchback Timing	Select the required timing from the drop-down list. The options include <i>Delayed</i> , <i>Graceful</i> , <i>Immediate</i> and <i>Scheduled</i> .
Switchback uptime-delay	The uptime delay specified in minutes. The default is ten (10) minutes.
Switchback Schedule	Specify the switchback schedule time. The time is specified in the format hh:mm.
Type of DTMF Relay	Select the required DTMF Relay from the drop-down list. The options include, <i>Current GW Config</i> , <i>NSE</i> , <i>NTE-CA</i> , <i>NTE-GW</i> , and <i>Out of Band</i> .
Fax Mode	Select the required fax mode from the drop-down list.
Modem Passthrough	Select the checkbox (if required) to enable modem passthrough.
Supplementary Services	Select to enable Supplementary Services, including voicemail, call forwarding, conferencing and speed dials to be managed at location level as analog line features. Only available for SCCP analog gateways.

H.323 Protocol

Procedure

H.323 Gateway Configuration

H.323 gateways are configured in the system via the H.323 Gateway Configuration screen.

To configure a H.323 gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name* (active text link) of the gateway that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Complete all of the required fields and click the **Submit** button. The following fields are available when configuring a H.323 Gateway:

The gateway is configured.

Field	Description	Notes
Device Information:-		
Name	Name of the device currently being modified.	This field cannot be updated via this page.
Protocol	Protocol of the device currently being modified, that is H.225 / H.323.	This field cannot be updated via this page.
IP Address	IP address of the device currently being modified	This field cannot be updated via this page.
IP Address (alternate)	Alternate IP Address of the device currently being modified	This field cannot be updated via this page.
NAT IP Address	NAT IP Address of the device currently being modified	This field cannot be updated via this page.
Device Settings:-		
Device Pool	The device pool to which the current device is assigned.	Select from the drop-down list.
Call Classification	Used to specify if calls are classified as <i>onnet</i> or <i>offnet</i> . Select the required value from the drop-down list.	This is a mandatory field. If you would prefer to use the system default, select the <i>use system default</i> option.
Packet Capture Mode	Used to specify the packet capture mode. Options include <i>Batch Processing mode</i> and <i>None</i> . Select the required value from the drop-down list.	This is a mandatory field.
Gateway Voice Interface	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets.	This is a mandatory field.
Tunneled Protocol	Used to select the required tunnel protocol. Select the required value from the drop-down list.	This is a mandatory field.
Signaling Port	Enter the required signaling port into the text field.	This is a mandatory field.

Field	Description	Notes
Media Resource Group List	Select the required Media Resource Group List from the drop-down list.	Media Resource Group List s cannot be added here, please ensure the required list has been configured before attempting to configure a gateway.
MLPP Domain ID	Enter the MLPP domain ID	-
Retry Video Call as Audio	Select this checkbox if you would like the system to redial video calls as an audio call.	-
Packet Capture Duration	Specify the required packet capture duration.	-
sRTP Allowed	Select this checkbox if you would like to enable the use of sRTP for this gateway.	-
Wait for Far End H.245 Terminal Capability Set	Select this checkbox if you would like the gateway to wait to establish the far end terminals capabilities.	-
Media Termination Point Required	Select this checkbox if the gateway requires a media termination point.	Determines whether or not a Media Termination Point (MTP) is used to implement features that H.323 does not support (such as hold and transfer).
Inbound Calls:-		
Significant Digits	Use the drop-down list to specify the significant digits for this gateway, alternately, select the <i>All</i> option.	This is a mandatory field. Significant digits are counted from the right (last digit) of the number called.
Enable per port COS	Select this checkbox to allows per port COS (and the analog gateway COS) to be activated on individual ports.	-
Calling Search Space	Select the appropriate calling search space from the drop-down list.	A calling search space specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.
AAR Calling Search Space	Select the required AAR calling search space for the device to use when it performs automated alternate routing (AAR) from the drop-down list.	The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	This is used to specify the prefix digits that are appended to the called party number on incoming calls. Specify the required Prefix DN using the provided text field	-

Field	Description	Notes
Redirecting Number IE Delivery - Inbound	Select this checkbox to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.	Redirecting Number IE is for voice-messaging integration only. Note The default setting is to leave this checkbox unchecked.
Enable Inbound FastStart	Select this checkbox to enable the FastStart call connections.	Note For inter cluster calls, the <i>Enable Inbound FastStart</i> checkbox must be selected for all clusters.
Outbound Calls:-		
Calling Party Selection	Any outbound call on a gateway can send directory number information. Use the drop-down list to specify which number is sent.	This is a mandatory field.
Calling Party Presentation	Use the drop-down list to specify whether the calling party phone number is displayed or restricted.	This is a mandatory field.-
Called party IE number type unknown	Use the drop-down list to select the format for the number type in called party directory numbers.	This is a mandatory field.
Calling party IE number type unknown	Use the drop-down list to select the format for the number type in calling party directory numbers.	This is a mandatory field.
Called Numbering Plan	Use the drop-down list to select the format for the called numbering plan.	This is a mandatory field.
Calling Numbering Plan	Use the drop-down list to select the format for the calling numbering plan.	This is a mandatory field.
Caller ID DN	Enter the pattern that you would like to use for calling line ID.	Field accepts 0 to 24 digits.
Display IE Delivery	Select this checkbox to enable delivery of the display IE in SETUP, CONNECT, and NOTIFY messages for the calling and called party name delivery service.	-
Redirecting Number IE Delivery - Outbound	Select this checkbox to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager (Unified CM).	The Redirecting Number IE is for voice-messaging integration only. Note Default leaves the checkbox unchecked.
Enable Outbound FastStart Codec	Select this checkbox to enable the H.323 FastStart feature on outgoing calls.	-

Field	Description	Notes
Codec For Outbound FastStart	Using the drop-down list provided, select the codec for use with the H.323 device for an outbound FastStart call.	-
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.	<p>Select the required value from the drop-down list.</p> <p>Note</p> <p>Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as <i>None</i> for the device pool and you select the <i>Use device pool calling party transformation CSS</i> checkbox (see below) in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</p>
Use device pool calling party transformation CSS	Select checkbox if required.	Checkbox selected = uses the device pool's calling party transformation CSS.
Called Party Transformation CSS	Select the Called Party Transformation CSS that contains the called party transformation patterns that should be applied to calls routed through the trunk.	<p>This is a mandatory field. Select the required value from the drop-down list.</p> <p>You can also leave this set to <i>None</i> and use the Called Party Transformation CSS assigned to the device pool by selecting the <i>Use device pool called party transformation CSS</i> checkbox (see below).</p>
Use device pool called party transformation CSS	Select checkbox if required.	Checkbox selected = uses the device pool's called party transformation CSS.

SIP Protocol

When using the SIP protocol, please take note of the following:

- The SIP protocol is only supported for Cisco Unified Communications Manager (Unified CM) 6.1. and 7.1
- The DTMFSignalingMethod setting is not supported by the system for Unified CM 6.1. If using a Unified CM 6.1, please configure this setting manually on the Unified CM.
- The SIP protocol only supports FXS type ports
- Only one SIP gateway may be added to each device
- When adding a SIP gateway, the only Gateway Function that may be selected is Analog.

SIP gateways are configured in the system via the SIP Gateway Configuration screen.

Procedure

SIP Gateway Configuration

To configure a SIP gateway:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Name* (active text link) of the gateway that you would like to modify.
- Step 4** Click the **Gateway Hardware Configuration** button.
- Step 5** Complete all of the required fields and click the Submit button. The following fields are available when configuring a SIP Gateway:

The gateway is configured.

Field	Description	Notes
Device Information:-		
Name	Name of the device currently being modified.	This field cannot be updated via this page.
Description	Description of the device currently being modified.	This field cannot be updated via this page.
Protocol	Protocol of the device currently being modified.	This field cannot be updated via this page.
IP Address	IP address of the device currently being modified	This field cannot be updated via this page.
IP Address (alternate)	Alternate IP Address of the device currently being modified	This field cannot be updated via this page.
IP Address B	This IP address is available for use by Gateways when communicating with the Unified CM server. A Gateway option allows the user to specify whether the normal IP Address or this address is used. This allows support for various NAT configurations. See the IOS Gateways Guide for details on how to use these settings/options.	This field cannot be updated via this page.
Device Settings:-		
Device Pool	The device pool to which the current device is assigned.	Select from the drop-down list.
Gateway Voice Interface	This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets.	This is a mandatory field but cannot be updated via this page.
Common Device Configuration	Specify the common device configuration	-

Field	Description	Notes
Call Classification	Used to specify if calls are classified as <i>onnet</i> or <i>offnet</i> . Select the required value from the drop-down list.	This is a mandatory field. If you would prefer to use the system default, select the <i>use system default</i> option.
Media Resource Group List	Select the required Media Resource Group List from the drop-down list.	Media Resource Group Lists cannot be added here, please ensure the required list has been configured before attempting to configure a gateway.
Location	The current location related to the device.	This field cannot be updated via this page.
Packet Capture Mode	Used to specify the packet capture mode. Options include <i>Batch Processing mode</i> and <i>None</i> . Select the required value from the drop-down list.	This is a mandatory field.
Packet Capture Duration	Specify the required packet capture duration.	-
Media Termination Point Required	Select this checkbox if the gateway requires a media termination point.	Determines whether or not a Media Termination Point (MTP) is used to implement features that SIP does not support.
Retry Video Call as Audio	Select this checkbox if you would like the system to redial video calls as an audio call.	-
Unattended Port	Select this checkbox if this is going to be an unattended port.	-
sRTP Allowed	Select this checkbox if you would like to enable the use of sRTP for this gateway.	-
Trusted Relay Point	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>On</i> and <i>Off</i> .	-
Call Routing Information:-		
Remote-Party-Id	Select this checkbox if you would like to utilize <i>Remote-Party-Id</i> .	-
Asserted-Identity	Select this checkbox if you would like to enable <i>Asserted-Identity</i> .	-
Asserted-Type	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>PAI</i> and <i>PPI</i> .	This is a mandatory field.
SIP Privacy	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>ID</i> and <i>ID Critical</i> .	This is a mandatory field.
MLPP Domain ID	Select the required value from the drop-down list.	-
Inbound Calls:-		

Field	Description	Notes
Significant Digits	Use the drop-down list to specify the significant digits for this gateway, alternately, select the <i>All</i> option.	This is a mandatory field. Significant digits are counted from the right (last digit) of the number called.
Connected Line ID Presentation	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
Connected Name Presentation	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
Enable per port COS	Select this checkbox to allow per port COS (and the analog gateway COS) to be activated on individual ports.	-
Calling Search Space	Select the appropriate calling search space from the drop-down list.	A calling search space specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed.
AAR Calling Search Space	Select the required AAR calling search space for the device to use when it performs automated alternate routing (AAR) from the drop-down list.	The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
Prefix DN	This is used to specify the prefix digits that are appended to the called party number on incoming calls. Specify the required Prefix DN using the provided text field	-
Redirecting Diversion Header Delivery - Inbound	Select this checkbox if Redirecting Diversion Header Delivery - Inbound	-
Connected Party Transformation CSS	Allows you to transform the connected party number on the device in order to display the connected number in another format, such as a DID or E164 number. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device.	If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use device pool connected party transformation CSS	Select this checkbox to use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device.	If you do not select this checkbox, the device uses the Connected Party Transformation CSS that is configured for this device.
Outbound Calls:-		

Field	Description	Notes
Calling Party Selection	Any outbound call on a gateway can send directory number information. Use the drop-down list to specify which number is sent.	This is a mandatory field.
Calling Line ID Presentation	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
Calling Name Presentation	Select the required value from the drop-down list. Available options include <i>Default</i> , <i>Allowed</i> and <i>Restricted</i> .	This is a mandatory field.
Caller ID DN	Enter the pattern that you would like to use for calling line ID	Field accepts 0 to 24 digits.
Caller Name	Specify the required value in the provided text field.	-
Redirecting Diversion Header Delivery - Outbound	Select this checkbox if Redirecting Diversion Header Delivery - Outbound	-
Calling Party Transformation CSS	Allows you to localize the calling party number on the device. Select from the drop-down list.	This is a mandatory field. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use device pool calling party transformation CSS	Select this checkbox to use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device.	If you do not select this checkbox, the device uses the Calling Party Transformation CSS that you configured in the drop-down list (see field above).
Called Party Transformation CSS	Allows you to localize the called party number on the device. Select from the drop-down list.	This is a mandatory field. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device.
Use device pool called party transformation CSS	Select this checkbox to use the Called Party Transformation CSS that is configured in the device pool that is assigned to this device.	If you do not select this checkbox, the device uses the Called Party Transformation CSS that you configured for this device in the drop-down list (see field above).
Redirecting Party Transformation CSS	Allows you to localize the redirecting party number on the device. Select from the drop-down list.	This is a mandatory field. Make sure that the Redirecting Party Transformation CSS that you choose contains the redirecting party transformation pattern that you want to assign to this device.
Use device pool redirecting party transformation CSS	Select this checkbox to use the Redirecting Party Transformation CSS that is configured in the device pool that is assigned to this device.	If you do not select this checkbox, the device uses the Redirecting Party Transformation CSS that you configured for this device in the drop-down list (see field above).

Field	Description	Notes
SIP Information:-		
Destination Address	The destination address of the gateway.	This is a mandatory field but cannot be modified via this page.
Destination Address is an SRV.	Select this checkbox if the destination address is an SRV	-
Destination Port	Specify the required port of the gateway.	This is a mandatory field.
MTP Preferred Originating Codec	The MTP Preferred Originating Codec for the gateway.	This field cannot be modified via this page.
Presence Group	Specify the presence group for the gateway.	This is a mandatory field.
SIP Trunk Security Profile	Specify the SIP Trunk Security Profile.	This is a mandatory field.
Rerouting Calling Search Space	Select the required value from the drop-down list.	-
Out-Of-Dialog Refer Calling Search Space	Select the required value from the drop-down list.	-
SUBSCRIBE Calling Search Space	Select the required value from the drop-down list.	-
SIP Profile	Specify the required SIP profile.	This is a mandatory field.
DTMF Signalling Method	Select the required value from the drop-down list.	This is a mandatory field.

Download Command List

To download a copy of the command list, click the **Download** button. The browser should display a *Save as ... / Open with ...* dialog box.

If the extra details were displayed in the command list, then each block of commands is preceded by an IOS comment containing the action name.

Note

Download behavior can differ amongst browsers. If you experience any difficulty while downloading command lists, consider one of the following options:

If an error is returned when attempting to download the file, try clicking the **View in new window** button and then browse to *File > Save As* in your browser. After saving the file to a location of your choice, you can view the file as usual.

Alternatively, click the **Download** button and then click the **Open** option. From within the browser, browse to *File -> Save As*.

Exporting IOS Commands

Procedure

Exporting the Command List Without Editing it

The list of commands may be exported to an external FTP server. To do this:

Step 1 Select the **Export** button on the command list screen

Step 2 Complete all of the required fields

The following fields are available:

Field	Description
Server name or IP address	The name or IP address of the FTP server you will be connecting to.
Login name	Login (user) name for the FTP server, this is not related to your system login.
Password	Password for FTP server.
File name	The name of the file to be saved on the remote FTP server.
SFTP	Select this checkbox if you are going to be using an SFTP connection.
Passive mode FTP	Select this checkbox if you are going to be using a Passive mode FTP connection.

Step 3 To export all the commands to the remote server, click the **Export All** button. To export only those commands since the most recent export (commands displayed in red), click the **Export Recent** button.

Note

The **Export Recent** button will not appear if there are no recent commands present.

Procedure

Edit and Export Command List

The list of commands may be edited before being exported to an external FTP server. To do this:

Step 1 Click the **Export & Edit** button on the command list screen.

Step 2 Complete all of the required fields.

Step 3 Once you have finished editing the commands, click the **Export** button to export the commands to the remote server.

The following fields are available:

Field	Description
Server name or IP address	The name or IP address of the FTP server you will be connecting to.
Login name	Login (user) name for the FTP server, this is not related to your system login.
Password	Password for FTP server.
File name	The name of the file to be saved on the remote FTP server.
SFTP	Select this checkbox if you are going to be using an SFTP connection.
Passive mode FTP	Select this checkbox if you are going to be using a Passive mode FTP connection.

Adding a Gateway Role to the IOS Device

The Gateway function essentially a role of an IOS device, and is effectively a network point that acts as an entrance to another network.

Router PSTN connectivity is generically referred to as voice gateway functionality, offering a gateway for voice over IP (VoIP) calls to, and from, traditional analog or digital PSTN or private branch exchange (PBX) calls. You can use a voice gateway to connect to PSTN central office (CO) switches, private branch exchanges (PBXs), Key Systems, time-division multiplexing (TDM)-based interactive voice response (IVR) systems, traditional TDM-based voice mail systems, and any other legacy (non-IP) voice processing or telephone equipment.

The following gateway protocols are supported:

- MGCP
- SCCP
- SIP
- H323
- MGCP-DPNSS
- MGCP-Q931

The following gateway port types are supported:

- FXS
- FXO
- E1
- T1
- PRI
- E&M
- BRI

Gateways can have the following functions:

- Analog
- PSTN Local
- Legacy
- PSTN Central

Gateway roles can be added manually or via the Gateway Wizard. For information on adding gateway roles using the wizard, see [IOS Gateway Wizards on page 221](#).

Procedure

To add a Gateway role to an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.

- Step 2** Select the *Device* (active text link) to which you want to add a Gateway role.
- Step 3** Select the *Gateway* checkbox in the *Device Roles* section of the screen and then click the **Modify** button.
- Step 4** Click the **Add** button adjacent to the Gateway device role in the *Device Roles* section. Mandatory fields include:

Field	Notes	Remarks
Device Details		
Host name	For information purposes only.	Cannot be modified.
Description	For information purposes only.	Cannot be modified.
Single Location Only	For information purposes only.	Cannot be modified.
Location	For information purposes only.	Cannot be modified.
Gateway Details		
Name	The name of the Gateway role.	This is a mandatory field.
Description	Description of the Gateway role.	-
IP Address	The IP Address for the gateway role.	<p>This is a mandatory field.</p> <p>Note</p> <ul style="list-style-type: none"> • If the Provider preference setting AllowDuplicateIpAddresses is enabled (see Available Preferences and Settings on page 934 if required), a Gateway role can share its IP Address with another Gateway role (as long as the other Gateway role is within a different Customer). • The gateway role IP address is locked and may not be modified once the hardware configuration is setup (that is, the Gateway has been loaded into the PGW). The IOS device and gateway role IP addresses may be different and the IOS device IP address remains configurable as this isn't the IP address used in the call agent.
IP Address (Alternate)	An optional, alternate, IP Address within the provider.	-

Field	Notes	Remarks
IP Address B	This is the IP address that other devices, for example Unified CMs, use when communicating with the Gateway. The use of this field is described by the option that follows.	This is a mandatory field when the <i>Unified CM to use Gateway IP B</i> option is selected. Note This IP Address needs to be provided in the standard IP address format.
Unified CM to use Gateway IP B	This causes Unified CMs communicating with this device to use the IP address configured in <i>IP Address B</i> on the Gateway.	Note This option allows communication from the Unified CM to the Gateway via a NAT Boundary. Details on how to utilize this in a specific scenario are described in the <i>IOS Gateways Guide</i> .
Gateway to Use Unified CM IP B	This Gateway uses the Unified CM IP address configured in the <i>IP Address B</i> field on the Unified CM configuration screen.	Note This option allows communication from the Gateway to the Unified CM via a NAT Boundary. Details on how to utilize this in a specific scenario are outlined in the <i>IOS Gateways Guide</i> .
Protocol	The protocol for the gateway.	This is a mandatory field. The IOS Device may be configured with multiple gateway roles but is limited to one gateway role per protocol.
Supplementary Services	Supplementary Services, including voicemail, call forwarding, conferencing and speed dials can be enabled to be managed at location level as analog line features.	Only available for SCCP analog gateways. Select to enable.

Step 5 Click the **Next** button.

Section	Field	Remarks
Gateway Details	Type and name of the device to which the gateway connects.	Select the type and name of the device to which the gateway connects.

Step 6 Click the **Next** button.

Within the *Gateway Functions* section, select the required functions of the gateway (see table below for supported gateway functions).

Protocol	Connect Device Type	Gateway Functions				
		PSTN Central	PSTN Local	Analog	Legacy	
MGCP	IPPBX	Y	Y	Y		
	Transit Switch				Y	
SCCP	IPPBX	Y		Y		
H.323	IPPBX	Y	Y	Y		Y
SIP	IPPBX		Y	Y		Y

Step 7 Click the **Add** button.

PGW Pre and Post Functions

This feature allows MML commands to be specified which are run outside of a provisioning session. The Pre commands are run before the provisioning session is started and the Post Commands are run after the provisioning session is finished. This gives the flexibility to run any MML commands required during a model (e.g. commands to take thing OOS for a mod, or IS after an Add, etc).

For example, if a component needs to be modified, we need to take it OOS (out of service), make the change via the relevant commands, and then put it back IS (In Service). In this example we would include a "Pre" model, take the component out of service, run the appropriate MML, do a PROV-DPLY or PROV-CPY, and then run the "Post" function to put the relevant component back in service. To make use of this functionality in the PGW model, the text "-Pre" or "-Post" is added to the end of the MML Script Name (e.g. DelQ931-Pre or ModQ931Trunk-Post).

Note

The pre and post logic does ignore PGW errors indicating the element is already in that state (i.e. trying to set something OOS which is already in that state).

Supported MML Scripts

This is currently supported with the legacy PBX transactions in the PGW model (no support in the TimesTen model).

Transaction Failures and Rollback

If a failure occurs during the PGW provisioning session this is the behavior with regards to the Pre and Post models.

If a pre-model exists and one of the commands in the Pre model fails, the transaction stops at that failure and the errors are output to the screen. The main model and Post model are not run. This is due to the fact that the main model will likely fail if Pre commands were required so there isn't any point in continuing. Any successful commands issues from the Pre model will need to be undone on the PGW if required.

If the pre succeeds (or doesn't exist) and a failure occurs during the main configuration session, then the transaction stops at that failure and any errors are output to the screen. The post model is not run. Any commands issued in the Pre model will need to be undone on the PGW if required.

If the pre succeeds (or doesn't exist) and the main model succeeds, then there is an error in the post model, the transaction does NOT fail however any errors from the post model are output to the

transaction. This is due to the fact that the types of commands in the Post aren't configuration and won't be crucial to the provisioning. Any failed Post commands can be resolved manually on the PGW if required.

The approach to rollback outlined above was taken as depending on the transaction, the Post may not be a rollback for the Pre, etc (i.e. an Add or Del). This type of failure is rare in production environments but should be considered when putting together the models and operational processes.

Legacy Gateways

The Legacy Gateway functionality in the system provides the ability to create legacy gateways and connect them to a transit switch (Cisco PGW). The system configures the gateway and related trunks on the IOS device and the related dial plan. The main function of the legacy gateways in the system is for connectivity of unmanaged locations to legacy PBX's. Once setup and connected to a transit, they can be associated with a location to provide the connectivity for that legacy site to the Cisco HCS architecture.

This section covers the setup and management of the legacy gateways and connecting them to an unmanaged location. The IOS device management functionality is accessed by browsing to *Network > IOS Devices* in the system.

Search Functionality

The following search criteria are available for IOS Devices:

- Host Name
- IP Address
- Role

The following columns are available on the Search Results page:

- Host Name
- IP Address
- Single Location
- Supported Roles

Adding an IOS Device

Procedure

To add an IOS device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button.
- Step 3** The following details need to be provided in the *Device Details* section of the *Add IOS Device* screen:
 - **Host Name:** This is a mandatory field and must be unique.
 - **Description:** An optional short description of the IOS device being added.

- **Country:** This is a mandatory field. The country specific details to be applied to the device. Select the relevant Country from drop-down list. The default country is the country of the current provider.
- **Select Owner:** This is a mandatory field, select the relevant Provider /Reseller/Building/ Customer/ Division/Location.
- **Single Location Only:** Checkbox to enable or disable.
- **Select Location:** Select relevant Unmanaged Location from drop-down list.

The following details need to be provided in the *Connectivity Details* section of the *Add IOS Device* screen.

- **IP Address:** This is a mandatory field and must be unique.
- **IP Address (Alternate):** An optional secondary IP address.
- **IP Domain:** An optional Domain Name.
- **Cisco User ID required:** An optional checkbox if username is required to access IOS device.
- **Config User Password:** An optional field if username's password is required for IOS device.
- **Config Password:** This is a mandatory field, required for configuration password for IOS device.
- **Enable Password:** This is a mandatory field, required for enable password for IOS device.
- **Software Version:** Drop-down list of relevant IOS device version.
- **Manual Configuration Mode:** An optional checkbox to place IOS device in manual or live mode.
- **Email address for Manual activation:** This option is mandatory if the Manual Configuration Mode option has been selected.
- **Network Monitoring active:** An optional checkbox.
- **Detailed trace file of configuration sessions:** An optional checkbox.
- **Encrypt configuration sessions:** An optional checkbox if SSH is used to access the IOS device.

The following details need to be provided in the *Device Roles* section of the *Add IOS Device* screen:

- **Gateway:** Checkbox to select a Gateway device role for the IOS device and an **Add** button to complete the Add IOS device.
- **Media Resources:** Checkbox to select a Media Resource device role for the IOS device and an **Add** button to complete the Add IOS device.
- **SRST:** Checkbox to select a SRST device role for the IOS device and an **Add** button to complete the Add IOS device.

Step 4 Click the **Add** button.

Adding a Gateway Role

Procedure

To add a gateway role:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Click the **Add** button next to the relevant Gateway in the *Device Roles* section of the *IOS Device* screen.
- Step 3** The following details need to be provided in the **Gateway Details** section of the Add form:
- **Name:** The name of the IOS gateway. This field is mandatory.
 - **Description:** An optional description of the gateway.
 - **IP Address:** This is a mandatory field and must be unique. This is the IP address used to configure the Gateway itself and could be different to the IP address defined on the IOS device screen (often it is the same).

Note

If the Provider preference setting *Allow DuplicateIpAddresses* is enabled, an IOS Gateway can share its IP Address with another IOS Gateway (as long as the other IOS Gateway is within a different Customer). Note also that the gateway IP is used for the PGW and may be different from the IOS device IP address. The gateway IP address is locked once the hardware configuration is setup (i.e. the Gateway has been loaded into the PGW).

- **IP Address (Alternate):** A secondary IP address for the gateway. This must be a unique IP Address within the provider.
 - **IP Address B:** This is the IP address that other devices, for example Unified CMs, use when communicating with the Gateway. The use of this field is described by the option that follows. This is a mandatory field when the *Unified CM to use Gateway IP B* option is selected.
 - **Unified CM to use Gateway IP B:** This causes Unified CMs communicating with this device to use the IP address configured in *IP Address B* on the Gateway. This option allows communication from the Unified CM to the Gateway via a NAT Boundary. Details on how to utilize this in a specific scenario are described in the *IOS Gateways Guide*.
 - **Gateway to Use Unified CM IP B:** This Gateway uses the Unified CM IP address configured in the *IP Address B* field on the Unified CM configuration screen. This option allows communication from the Gateway to the Unified CM via a NAT Boundary. Details on how to utilize this in a specific scenario are outlined in the *IOS Gateways Guide*.
 - **Protocol:** Drop-down list of gateway protocols, choices are SCCP, H.225 and MGCP. Selecting a protocol is mandatory. When adding a Legacy gateway, select the MGCP option.
- Step 4** Click the **Next** button.
- Step 5** Complete the following.
- **MAC Address (12 Characters):** The MAC address of the gateway. An optional field, required only if protocol is SCCP. This field is limited to 12 characters.
 - **Supplementary Services:** Select to enable Supplementary Services, including voicemail, call forwarding, conferencing and speed dials to be managed at location level as analog line features. Only available for SCCP analog gateways, and is a mandatory field.
- Step 6** From the *Select Device* drop-down list, select the device you want to connect the gateway to. Valid options are IPPBX's or Transit switches. For Legacy Gateways, select the appropriate *Transit switch*.
- Step 7** Click the **Next** button.
- Step 8** Under the Gateway Functions section, if a Transit switch was chosen in the previous section, then the only option available is the "Legacy" role.
- Step 9** Enable the *Legacy* role then click the **Add** button.

Legacy Gateway Hardware Configuration

Procedure

To modify a gateways hardware configuration:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the Gateway *Name* (active text link).
- Step 3** Modify the required fields.

Note

The Legacy Protocol field consists of a drop-down list of protocols. Options include DPNSS and Q931.

- Step 4** Select a protocol then click the **Next** button. The *Legacy Configuration Details* section will now be displayed.

The *Configuration* section of the page displays the following information for DPNSS:

- **Gateway Type:** The gateway type as defined in the PGW. This value will be the name of an external node type and is used to specify the #GWTYPE# variable. This is a mandatory field, available options include: C1751, C1751_OLD, C1760, C1760_OLD, C2600, C2600_OLD, C2610XM, C2610XM_OLD, C2611XM, C2611XM_OLD, C2620XM, C2620XM_OLD, C2621XM, C2621XM_OLD, C2650XM, C2650XM_OLD, C2651XM, C2651XM_OLD, C2691, C2691_OLD, C3600, C3640, C3640A, C3660, C3725, C3725_OLD, C3745, C3745_OLD, C2801, C2811, C2821, C2851, C3825, C3845, AS5300, AS5350, AS5400, AS5850, and AS7200.
- **Gateway Voice Interface :** This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is a mandatory field.
- **Backhaul Port Number:** Text box to input port number .Default value is 9900 for DPNSS.

The *Configuration* section of the page displays the following information for Q931:

- **Gateway Type:** The gateway type as defined in the PGW. This value will be the name of an external node type and is used to specify the #GWTYPE# variable. This is a mandatory field, available options include: C1751, C1751_OLD, C1760, C1760_OLD, C2600, C2600_OLD, C2610XM, C2610XM_OLD, C2611XM, C2611XM_OLD, C2620XM, C2620XM_OLD, C2621XM, C2621XM_OLD, C2650XM, C2650XM_OLD, C2651XM, C2651XM_OLD, C2691, C2691_OLD, C3600, C3640, C3640A, C3660, C3725, C3725_OLD, C3745, C3745_OLD, C2801, C2811, C2821, C2851, C3825, C3845, AS5300, AS5350, AS5400, AS5850, and AS7200.
- **Gateway Voice Interface:** This field is used to specify the Gateway Voice Interface name and number. For example, GigabitEthernet0/0/0, FastEthernet0/1, or Loopback0. This information is used to identify the source interface for signaling and media packets. This is mandatory.
- **Backhaul Port Number:** Textbox to input port number. Default value is 7007 for Q931.
- **ISDN Protocol:** Drop-down list of protocols. Valid options are AT&T 41459, AT&T 41459 variant C2, BELL 1268, BELL 1268 variant C2, ETS 300 102, ETS 300 102 variant C2, QSIG, Q931(Default), Q931 AUSTRALIA, Q931 SINGAPORE
- **Call Reference Length:** Drop-down list. Valid options are 1 or 2(Default).

- Step 5** Click the **Modify** button to complete the configuration.

Adding Legacy Ports

On the IOS Gateway page, under the *Interface Details* section, select the *Gateway Hardware Configuration* link. Under the Legacy Ports section, click the **Add Port** button.

The *Add Legacy Port Summary* section of the page displays the following information:

- **Port Type:** Drop-down list. If gateway is DPNSS, then only E1 is available. If Q931, then both E1/T1 are available.
- **Port Number:** Textboxes to enter Slot/Sub-Unit/Port numbers. Slot/Port numbers are mandatory.
- **Add Range (optional):** Add Port Range is limited to 100 ports per transaction
- **Port Description :** An optional short description of the Legacy port being added

To complete the process, click the **Add** button.

Deleting Legacy Ports

Legacy Ports can only be deleted if they are deactivated, unallocated and unconfigured first.

Configuring Legacy Ports

To configure ports, click the **Configure** button under the *Legacy Ports* section of one of the ports.

The Port Configuration Details section of the page displays the following information:

- **Framing :** Drop-down list. For E1, CRC4 or Non CRC4 (Default) is available. For T1, we have ESF (Default) or SF.
- **Clock Source :** Drop-down list. Valid options are Line(Default) and Internal
- **Line Coding:** Drop-down list. For E1, AMI or HDB3 (Default) is available. For T1, we have B8ZS (Default) and AMI.
- **Pri-Group Timeslots:** This field is read only. For E1, it is set to 1-31, for T1, it is set to 1-23
- **Interface Serial:** This field is read only. For E1, it is set to 15, for T1, it is set to 23
- **ISDN Switch Type:** If gateway is DPNSS, field is set read-only to primary-dpnss. If gateway is Q931, we have a drop-down listing primary-net5, primary-ntt, primary-4ess, primary-5ess, primary-dms100 and primary-ni.
- **Circuit Selection Method:** Drop-down box listing Least Idle, Most Idle (Default), Ascending, Descending, Random, Even Descending, Odd Descending, Even Ascending, Odd Ascending, Cyclic Ascending, Cyclic Descending and ITU2.
- **Call Collision Handling:** Drop-down box listing Release both calls, Network has priority, PBX has priority.

Click the **Add** button to complete the port configuration.

Allocating Legacy Ports

To allocate ports, under the legacy interfaces section on the IOS Gateway main page, click the **Port Allocation** button. On the *IOS Gateway Legacy Port Allocation page*, the *Legacy Port Allocation* section of the page displays the following information:

- **Select Location:** Drop-down box listing the Unmanaged Location for allocation

- **Allocate:** Checkbox to select or deselect
- **Port Number:** Displays Slot/Subunit/Port info
- **Port Type:** Displays port type E1 or T1
- **Description:** Displays port description if set

Select the port/s you want to allocate then click the **Allocate** button.

Legacy Gateway Activation

To complete the activation process, navigate to *Location Administration > Telephony > Legacy Gateways* in the system.

The *Location Details* section of the page displays the following:

- **Location ID:** Read-only field denoting the Location ID stored in the system.
- **Call Limit:** Mandatory text field required to set the call limit numeric value for the Unmanaged Location. This value is modifiable after activation.

The *Location Trunk Details* section of the page displays the following:

- **Default DN:** Mandatory text field required to set the default directory number value for the Unmanaged Location. Numeric only. This value is modifiable after activation.
- **Own Routing Number:** Mandatory numeric field used to set the own routing number value for the Unmanaged Location, DPNSS gateways only. This value is modifiable after activation.

The *Legacy Interface Details* section of the page displays the following under *Available interfaces*:

- **Gateway Name:** Displays name of Legacy Gateway
- **Connected Device:** Displays name of connected Transit switch
- **Protocol:** Displays legacy protocol, DPNSS or Q931
- **Port Number:** Displays legacy port in the slot/subunit/port format
- **Port Type:** Displays port type, E1 or T1
- **Priority:** Mandatory text field required to set trunk priority value. Numeric only.
- **Checkbox:** To select or deselect the appropriate trunk.

Select the appropriate trunk/s, give them a priority value, then click the **Submit** button. This will invoke an IOS driver call to the IOS device to configure the appropriate gateway and trunk configuration as well as a PGW driver call to configure the appropriate gateway and trunk configuration on the Transit switch.

For DPNSS, the *Driver_PSTN_Gateway* calls the *AddMGCP-DPNSS* and *AddVoiceTrunkPRI-MGCP-DPNSS* model name from the IOS Device Model. The *Driver_TransitSwitch* calls the *AddDPNSS*, *AddDPNSSTrunk* and *MaintainLocationLegacyGW-Activate* MML Script Name from the PGW Model. The *AddDPNSS* variables are substituted into the *#GWBLOCK#* per Gateway instance upon activation. The *AddDPNSSTrunk* variables are substituted into the *#TRUNKBLOCK#* per Trunk of the Gateway upon activation.

For Q931, the *Driver_PSTN_Gateway* calls the *AddMGCP-Q931* and *AddVoiceTrunkPRI-MGCP-Q931* model name from the IOS Device Model. The *Driver_TransitSwitch* calls the *AddQ931*, *AddQ931Trunk* and *MaintainLocationLegacyGW-Activate* MML Script Name from the PGW Model. The *AddQ931* variables are substituted into the *#GWBLOCK#* per Gateway instance upon

activation. The *AddQ931Trunk* variables are substituted into the *#TRUNKBLOCK#* per Trunk of the Gateway upon activation.

Legacy Gateway Deactivation

To complete the deactivation process, navigate to *Location Administration > Telephony > Legacy Gateways* in the system.

Select all the trunks, click the **Submit** button. This will invoke an IOS driver call to the IOS device to remove the gateway and trunk configuration as well as a PGW driver call to remove the gateway and trunk configuration on the Transit switch.

For DPNSS, the *Driver_PSTN_Gateway* calls the *DelMGCP-DPNSS* and *DelVoiceTrunkPRI-MGCP-DPNSS* model name from the IOS Device Model. The *Driver_TransitSwitch* calls the *DelDPNSS*, *DelDPNSSTrunk* and *MaintainLocationLegacyGW-Deactivate* MML Script Name from the PGW Model. The *DelDPNSSTrunk* variables are substituted into the *#TRUNKBLOCK#* per Trunk of the Gateway upon deactivation. The *DelDPNSS* variables are substituted into the *#GWBLOCK#* per Gateway instance upon deactivation.

For Q931, the *Driver_PSTN_Gateway* calls the *DelMGCP-Q931* and *DelVoiceTrunkPRI-MGCP-Q931* model name from the IOS Device Model. The *Driver_TransitSwitch* calls the *DelQ931*, *DelQ931Trunk*, and *MaintainLocationLegacyGW-Deactivate* MML Script Name from the PGW Model.

The *DelQ931Trunk* variables are substituted into the *#TRUNKBLOCK#* per Trunk of the Gateway upon deactivation. The *DelQ931* variables are substituted into the *#GWBLOCK#* per Gateway instance upon deactivation.

Connect Legacy Trunk

To connect additional trunks, navigate to *Location Administration > Telephony > Legacy Gateways*. Under *Available interfaces*, select the appropriate trunk/s, give them a priority value then click the **Connect** button. This will invoke an IOS driver call to the IOS device to configure the trunk configuration as well as a PGW driver call to configure the appropriate trunk configuration on the Transit switch.

- For DPNSS, the *Driver_PSTN_Gateway* calls the *AddVoiceTrunkPRI-MGCP-DPNSS* model name from the IOS Device Model.
- For Q931, the *Driver_PSTN_Gateway* calls the *AddVoiceTrunkPRI-MGCP-Q931* model name from the IOS Device Model.

If it is the first trunk to be connected, it runs the *MaintainLocationLegacyGW-ConnectTrunk* mml script, which calls the *#GWBLOCK#*, *#TRUNKBLOCK#* and adds the following:

- Gateway
- Selected trunks
- Respective dial plan for DPNSS or Q.931 for the Unmanaged Location

If you are adding additional trunks to an already activated gateway with connected trunks, the *MaintainLocationLegacyGW-ConnectTrunk* mml model is run which calls the *#TRUNKBLOCK#* variable for *DPNSS* or *Q.931* trunks (i.e. *AddDPNSSTrunk* or *AddQ931Trunk*). The *#GWBLOCK#* is commented out.

Disconnect Legacy Trunk

To disconnect trunk(s), navigate to *Location Administration > Telephony > Legacy Gateways*. Under *Connected interfaces*, select the appropriate trunk/s then click the **Disconnect** button.

This will invoke an IOS driver call to the IOS device to remove the trunk configuration as well as a PGW driver call to remove the appropriate trunk configuration on the Transit switch.

- For DPNSS, the Driver_PSTN_Gateway calls the DelVoiceTrunkPRI-MGCP-DPNSS model name from the IOS Device Model.
- For Q931, the Driver_PSTN_Gateway calls the DelVoiceTrunkPRI-MGCP-Q931 model name from the IOS Device Model.

If all the trunks are disconnected, it runs the *MaintainLocationLegacyGW-DisconnectTrunk* mml script, which calls the #TRUNKBLOCK# and #GWBLOCK#, which deletes the following:

- Selected trunks
- The gateway(s)
- Respective dialplan for DPNSS or Q.931 for the Unmanaged Location

If you are disconnecting selective trunks of a gateway, but not all the trunks, the *MaintainLocationLegacyGW-DisconnectTrunk* mml model is run which calls the #TRUNKBLOCK# variable for DPNSS or Q.931 trunks (i.e. DelDPNSSTrunk or DelQ931Trunk). The #GWBLOCK# is commented out.

Modifying Activated Trunks settings

To modify trunk/s navigate to *Network > IOS Devices* in the system.

Select the IOS Device, under Gateway Details, select the **Gateway Name**, under Interface Details, select Gateway Hardware Configuration, and under Legacy Port, click the **Manage** button for the port you want to modify.

Any change/s made to the Framing, Clock Source, Line Coding, and ISDN Switch Type settings will issue a Mod VoiceTrunkPRI-DPNSS or AddVoiceTrunkPRI-Q931 as per the IOS Device Model for DPNSS or Q931 and will only make a change on the IOS Device. Any change/s made to the Circuit Selection Method and Call Collision Handling settings will issue a ModDPNSSTrunk or ModQ931Trunk as per the PGW Model for DPNSS or Q931 and will only make a change on the Transit switch.

Modifying Activated Legacy Gateways

To modify a Legacy Gateway, it needs to be deactivated first from the Unmanaged Location before making changes to the settings such as Gateway Type, Gateway Voice Interface and Backhaul Port Number.

Adding a Media Resources Role

Procedure

To add a hardware media resource role:

- | | |
|---------------|---|
| Step 1 | Browse to <i>Network > IOS Devices</i> . |
| Step 2 | Click the Add button. |
| Step 3 | <p>The following details need to be provided in the Hardware Media Resource Details section of the Add form:</p> <ul style="list-style-type: none"> • Name: The name of the hardware media resource. This field is mandatory. • Description: An optional description of the gateway. • IP Address: This is a mandatory field and must be unique |

- **IP Address (Alternate):** An optional secondary IP address
- **MAC Address (12 Characters):** An optional field ,required only if protocol is SCCP
- **Protocol:** Drop-down list of gateway protocols, choices are SCCP, H.225 and MGCP. Selecting a protocol is mandatory. When adding a Legacy gateway, select the MGCP option.

Step 4 Click the **Next** button.

Step 5 From the *Select Device* drop-down list, select the device you want to connect the gateway to. Valid options are IPPBX's or Transit switches. For Legacy Gateways, select the appropriate *Transit switch*.

Step 6 Click the **Next** button.

Adding a SRST Role

See also: [SRST Role on page 355](#), as well as [The Survivable Remote Site Telephony \(SRST\) on page 355](#) if required.

Procedure

To add an SRST role to a Gateway:

Step 1 Browse to *Network > IOS Devices*.

Step 2 Click the **Add** button next to the required SRST device in the *Device Role* section on the *IOS Device* screen.

Step 3 The following details need to be provided in the *SRST Details* section on the *IOS Device - SRST Configuration* screen:

- **SRST Reference Name:** The name of the SRST reference added to Cisco Unified Communications Manager (Unified CM). This is a mandatory field.
- **Protocol:** Select the required protocol, which is used to select the correct model to run in order to provision the SRST device. This is a mandatory field. Cisco Unified Communications Domain Manager (CUCDM) only supports the SIP and H323 protocols.
- **IP Address:** The IP Address of the IOS device. This is a mandatory field.
- **SRST Port Number:** The port for the SRST connection. Used for the SRST reference in Unified CM. This is a mandatory field.
- **SIP Network/IP Address:** The SIP address or IP address of the SRST device. Used for the SRST reference in Unified CM. If an IP address is used, no NAT support is provided.
- **SIP Port Number:** Port number used if it is a SIP SRST connection. Used for the SRST reference in Unified CM. This is a mandatory field.
- **Is Secure?:** Checkbox to indicate secure SRST. Used for the SRST reference in Unified CM.
- **Max Conferences:** Value to indicate the max number of conferences the SRST device will support. Used to provide a variable for the IOS model for the ccm-fallback config. This is a mandatory field.
- **Max IP Phones:** Maximum phones supported by the SRST setup. Used to provide a variable for the IOS model for the Unified CM - fallback config. This is a mandatory field.
- **Allocated IP Phones:** This is a read only field showing the current number of phones that have been allocated to this SRST instance.

- **Max Directory Numbers:** Maximum directory numbers supported by the SRST setup. Used to provide a variable for the IOS model for the ccm-fallback config. This is a mandatory field.
- **Voicemail E.164 Fallback Number:** Used to dial the voicemail pilot from the PSTN when the IOS device is in active SRST mode.

The following details need to be provided in the *SRST Device Pool Details* section on the *IOS Device - SRST Configuration* screen:

- **Device Pool Config:** The name of the hardware media resource. This field is mandatory.
- **Create SRST Device Pool based on Device Pool:** This drop-down list displays all the device pools in the location. When the first SRST role is added to a Gateway in this location, this dropdown defaults to the Location's default device pool. If the administrator leaves this as is, then an SRST device pool is created based on the Location's default device pool (a copy is made, and the new SRST Reference is added.) Otherwise the administrator can choose a different device pool to use as a template for the new SRST device pool. Both "Location" and "SRST" device pools are listed in this dropdown list. Further SRST-device pool associations can be made via Add/Edit Device Pool at Location Administration -> Telephony -> Device Pools. Select the required device pool from the drop-down list of all device pools at the location.

If the *Custom* radio button was selected then complete the following additional custom fields:

- **Name:** The name of the device pool that you are creating. This is a mandatory field and must be unique.
- **Description:** A descriptive name for the device pool.
- **Device Pool Type:** SRST or Location
- **Device Pool Template:** Select the required device pool template from the drop-down list. This is a mandatory field.
- **Supported Streams:** The device pool capacity allocated to the device pool.
- **Call Manager Group:** Read-only field as specified in the device pool template.
- **Date/Time Group:** Specifies the date and time zone for the device.
- **Local Route Group:** Read-only field. None or from Global Settings as specified in the selected device pool template.
- **AAR CSS:** Read-only field. None or from Global Settings as specified in the device pool template.
- **AAR Group:** Read-only field. None or from Global Settings as specified in the device pool template.
- **Calling Party Transformation CSS:** Read-only field. None or from Global Settings as specified in the device pool template.
- **Called Party Transformation CSS:** Read-only field. None or from Global Settings as specified in the device pool template.

Step 4 Click the **Add** button when complete.

IOS Gateway - SRST Configuration

SRST configurations are added in the system via the *IOS Gateway - SRST Configuration* page.

Procedure

Add a Configuration

Follow these steps to add a SRST Configuration

- Step 1** Browse to *Network > IOS Devices*
- Step 2** Select the **Host Name** (active text link) that you would like to modify
- Step 3** Select the **Name** of the Gateway (active text link) that you would like to modify
- Step 4** Select the **Configure** button within the SRST section
- Step 5** Complete the required fields then select the **Add** button

The following fields are available via the *IOS Gateway - SRST Configuration* page:

Field	Description	Notes
Gateway Details:-		
<i>Name</i>	The name of the Gateway hosting this configuration	This field is for information purposes only and cannot be edited via this page.
<i>IP Address</i>	The IP Address of the Gateway hosting this configuration	This field is for information purposes only and cannot be edited via this page.
SRST Details:-		
<i>SRST Reference Name</i>	The reference name for the SRST	This field is for information purposes only and cannot be edited via this page.
<i>SRST Devicepool Name</i>	The devicepool of the SRST	This field is for information purposes only and cannot be edited via this page.
<i>SRST Port Number</i>	The port number of the SRST	The default value is 2000. This is a mandatory field.
<i>SIP Network/IP Address</i>	Enter the IP address of the server that the phones that are running SIP will use when in SRST mode	Note: You must configure the SIP Network/IP Address field and the SIP Port field for a SIP device to fall back to the SRST-enabled gateway. This is a mandatory field
<i>SIP Port Number</i>	The SIP port number	The default value specifies 5060. This is a mandatory field.
<i>Is Secure?</i>	Select this check-box if the SRST-enabled gateway contains a self-signed certificate.	Note: To remove the SRST certificate from the database and phone, un-check this check box, save your configuration and reset the relevant phones.
<i>Max Conferences</i>	Enter the maximum number of conferences allowed	This is a numeric This is a mandatory field
<i>Max IP Phones</i>	Enter the maximum number of IP phones allowed	This is a mandatory field
<i>Allocated IP Phones</i>	Enter the number of allocated IP phones	
<i>Max Directory Numbers</i>	Enter the maximum number of directory numbers allowed	This is a mandatory field

Field	Description	Notes
<i>Voicemail E.164 Fall-back Number</i>	Specify the Voicemail E.164 Fall-back Number	

Location Local Gateway Provisioning

This section covers provisioning dial plans for local gateways. Dial plan provisioning is performed after the gateway hardware has been configured on the system.

Dial Plan Provisioning interacts with the Cisco Unified Communications Manager and if needed the Gateway itself depending on the protocol used between the two.

The transactions for local gateways sub-transactions will be generated. The order of the sub-transactions may differ but they generally fall into the format of:

- Updating the database
- Updating the Cisco Unified Communications Manager
- If need be (in the case of a H323/H225 gateway) the update of the gateway.

During activation and deactivation of gateways, there are system features that might need to be applied to the gateways. These include features such as Emergency Number, Emergency Responder, Emergency CLI, Associate FNN Range and Forward User DDI. These features will be applied to a gateway the first time the gateway is activated and when the last port for the gateway is deactivated.

The Local Gateway Index

The *Local Gateway Dial Plan Provisioning* page can be accessed by browsing to *Location Administration > Telephony > (selecting the correct location) > Gateways*.

The *Gateway Index* page displays that available gateways and ports that can be activated or deactivated. The gateways and ports are grouped by their current activation status.

Activation of ports is performed by selected ports that are in a de-active state and selecting the **Activate** button. This will take the user to the *Advanced Dial Plan Configuration* page.

Deactivation of ports is performed by selected ports that are in an active state and click the **Deactivate** button.

Initial Provisioning of Dial Plan

When there is no dial plan currently provisioned for the selected location, a new dial plan will be created via the *Advanced Dial Plan Configuration* form. Creation of a new dial plan requires the following information:

- The Class of service
- The order of the gateways/ports
- The algorithm that will be applied to the order
- The port priority for H323/H225 ports

Note

With selection of H323 and H225 ports, they will be listed per gateway in the ordered list but will be assigned specific priority for each port.

When clicking the **Activate** button, the *AddLocationLocalGateway* transaction will be triggered. This spawns sub-transactions like *Driver_AddLocationLocalGateway*, *Driver_IPPBX* and *Driver_PSTN_Gateway* amongst others.

The *Driver_AddLocationLocalGateway* sub-transaction handles updates to the systems database.

The *Driver_IPPBX* sub-transaction handles the following (any CCM model lookups use the model name *AddLocationLocalGateway*):

- Adds a single route group for the location with the name RG-LGW-<location id> with the selected trunks/gateways in the selected order.
- Looks in the CCM model for the Route List details. It uses the route list sheet to determine the route lists required while the routegroup_routelist sheet provides the route groups to include in the list along with any settings.
- Adds any partitions, CSS, RP, TP and transformation patterns defined in the CCM model.
- Applies the COS to the port(s) or gateway(s).

The *Driver_PSTN_Gateway* sub-transaction is called once per H323 gateway (not called for MGCP/SCCP gateways).

The *AddLocationLocalGateway-H323* model is called for the default values to be applied to the gateway and the *AddLocationLocalGatewayTrunk-H323* model is called for all the ports being activated for this gateway.

For H323 and H225 ports the following additional transactions will execute:

- **AddEmergencyNumberOnGateway:** If an emergency number has been set up for this location it is applied on the gateway.
- **AddPSTNPubNumberOnGateway:** If a PSTN number has been set up for this location it is applied on the gateway.
- **AddELINonGateway:** If there is an emergency line number on this location then it gets applied on the gateway.
- **AddFNNRangesOnGateway:** If there are any full national number ranges on this location then it gets applied on the gateway.
- **AddFNNVMRangesOnGateway:** If there are any full national number voicemail ranges on this location, then they will be applied to the gateway.
- **EmergencyCLIONGateway:** If the location setting for Emergency CLI Preference is configured to derive from customer, the Emergency CLI Preference for the customer is applied to the gateway.
- **ModDDI4Rdn:** The FwdRedirectingExternalNumonCallFwd setting is enabled or disabled on the gateway depending on whether it has been enabled or disabled for the system.
- **ConnectLocalGW:** All active gateways in the location will be connected to the gateway being activated and vice versa. If more than one gateway is being activated, they will all be connected to each other in addition to being connected to the existing active gateways in the location.

Modification of the Current Dial Plan

When there is a dial plan active for the location, the user will be able to click the **Modify Dial Plan** button on the *Gateway Index* page, taking them to the *Advanced Dial Plan Configuration* form.

On clicking the **Modify** button, the *ModLocationLocalGateway* transaction will be kicked off. This transaction will determine the minimal changes required to perform the modification.

ModLocationLocalGateway will spawn sub-transactions like *Driver_ModLocationLocalGateway*, *Driver_IPPBX* and *Driver_PSTN_Gateway* respectively.

- The *Driver_ModLocationLocalGateway* sub transaction handles the updates to the systems database.
- The *Driver_IPPBX* sub-transaction will apply modifications to the current dial plan. This includes updating the route group order, the CSS applied to the GW/trunks, or the priority of the trunks on the H323 gateway. No CCM model call is made during this transaction.
- The *Driver_PSTN_Gateway* sub-transaction provisions each H323 port on the gateway using the model name *ModLocationLocalGatewayTrunk-H323*.

Activation of Additional Ports/Gateways

When there is a dial plan active for the location, the user will be able to select additional ports or additional gateways from the deactivated port section and click the **Activate** button. This will take the user to the *Advanced Dial Plan Configuration* Form.

When adding ports, the user is restricted from changing the Class of service and the device priority of existing H323/H225 protocol ports.

When clicking the **Add Trunk** button the *AddLocationLocalGatewayTrunk* transaction is kicked off. This transaction spawns sub-transactions like *Driver_AddLocationLocalGatewayTrunk*, *Driver_IPPBX* and *Driver_PSTN_Gateway* respectively.

The *Driver_AddLocationLocalGatewayTrunk* sub-transaction handles the updates to the systems database.

The *Driver_IPPBX* sub-transaction performs the following:

- Updates the route group with the new ports/gateways.
- Applies the Class Of Service to the new ports

The *Driver_PSTN_Gateway* sub-transaction provisions each new H323/H225 port on the gateway using the model name *AddLocationLocalGatewayTrunk-H323*.

The *Driver_PSTN_Gateway* sub-transaction is called once per H323 gateway (not called for MGCP/SCCP gateways). If a new gateway was added, then the *AddLocationLocalGateway-H323* model is called for the default values. The *AddLocationLocalGatewayTrunk-H323* model is called for all the ports being activated per gateway.

Deactivation of Ports

When there are activated ports for the current dial plan, the user will be able to deactivate them by selecting the port and clicking the **Deactivate** button. In the event that the user has not selected all of the active ports, the *DelLocationLocalGatewayTrunk* transaction will be kicked off.

If all the active ports were set to be deactivated then the dial plan will be removed and the transaction will be as listed in the *Removal of Dial Plan* section below:

- The *DelLocationLocalGatewayTrunk* transaction spawns sub-transactions such as *Driver_DelLocationLocalGatewayTrunk*, *Driver_IPPBX* and *Driver_PSTN_Gateway* respectively.
- The *Driver_DelLocationLocalGatewayTrunk* sub-transaction will update the systems database setting the selected ports to deactivated.
- The *Driver_IPPBX* sub-transaction will remove the selected port(s)/gateway(s) from the route group and reset their CSS back to None.

- The **Driver_PSTN_Gateway** sub-transaction will remove each H323/H225 port on from the gateway using the model name **DelLocationLocalGatewayTrunk-H323**.
- If all of the ports for a gateway are to be removed, the **DelLocationLocalGateway-H323** model is called.

For H323 and H225 ports, the following additional transactions will execute:

- **DelEmergencyNumberOnGateway:** The emergency number setting is disabled on the device.
- **DelPSTNPubNumberOnGateway:** The PSTN number setting is disabled on the device.
- **DelELINonGateway:** The emergency line number setting is disabled on the device.
- **DelFNNRangesOnGateway:** The full national number ranges are disabled on the device.
- **DelFNNVMRangesOnGateway:** The full national number voicemail ranges are disabled on the device.
- **ConnectLocalGW:** All active gateways in the location will be connected to the gateway being activated and vice versa. If more than one gateway is being activated, they will all be connected to each other in addition to being connected to the existing active gateways in the location.

Removal of Dial Plan

When there is an active dial plan, the user will be able to click the **Delete Dial Plan** button on the *Gateway Index* page. Deleting a dial plan can also be done by selecting all the active ports and selecting **Deactivate** on the *Gateway Index* page. The following will occur:

- The **DelLocationLocalGateway** transaction spawns sub-transactions like **Driver_IPPBX**, **Driver_PSTN_Gateway** and **Driver_DelLocationGateway**.
- The **Driver_PSTN_Gateway** sub-transaction removes the configuration of the ports from the gateway, using the model **DelLocationLocalGateway-H323** for the gateway and **DelLocationLocalGatewayTrunk-H323** for the ports.
- The **Driver_IPPBX** removes all the information created for the locations dial plan on Cisco Unified Communications Manager.
- The **Driver_DelLocationGateway** removes the configuration from the system's internal database.

Transit Switch Management

The following functionality is available via the Transit Switches section:

- [Transit Switch Management on page 304](#)
- [Selecting the Server Type to Add on page 94](#)
- [Add a PGW Server on page 306](#)
- [View and Modify a PGW Server on page 308](#)
- [PGW Server Tools on page 310](#)
- [Add a Technician Server on page 115](#)
- [Device Sets on page 347](#)
- [Add a Device Set on page 348](#)
- [Transit/Gatekeeper Management on page 320](#)

- [Transit/Transit Server Management on page 318](#)
- [Transit/Voicemail Server Management on page 319](#)
- [Manage a H.323 Signaling Interface on page 316](#)
- [HSI Management on page 312](#)
- [Add a HSI Interface on page 314](#)
- [Manage a H.323 Signaling Interface on page 316](#)

A Transit Switch provides four main functions:

- Network inter-connectivity for signal processes (Ss7)
- Advanced routing capabilities for call control
- Regulatory Functions , 911, Number Portability, and so on
- Billing record generation

Note

You must be at the Service Provider Administrator security level, or higher, to access Transit Switch Management.

From the Transit Switch Management screen, the following tools are accessible:

Tool/Task	Accessed Via	Description
Tools	Click the Tools button.	Opens a screen containing a list of available tools for the server.
Adding a Server	Click the Add button.	For more information, see Adding a Transit Switch .
Transit => Gatekeeper	Click the Transit => Gatekeeper button.	This screen enables you to manage connections between Transit Servers and Gatekeepers.
Transit => Transit	Click the Transit => Transit button.	This screen enables you to manage connections between a Transit Server and another Transit server.
Transit => VM Server	Click the Transit => VM Server button.	This screen enables you to manage connections between a Transit Server and a VM Server.
Associated Devices	Click the <i>Associated Devices</i> active text link.	For more information, see the Device Sets on page 347 help topic.

[Add a PGW Server on page 306](#)

For more information about the types of servers available, please select the relevant topic below:

- [Add a Technician Server on page 115](#)
- [Add a PGW Server on page 306](#)
- [Add a Technician Server on page 115](#)

[View and Modify a PGW Server on page 308](#)

Procedure

Deleting a Transit Switch

To delete a switch:

- Step 1** Browse to *Network > Transit Switches*.
 - Step 2** Select the *Name* (active text link) of the switch that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the switch is removed from the system.

[PGW Server Tools on page 310](#)

Procedure

Testing the Switch

To test a switch:

- Step 1** Browse to *Network > Transit Switches*.
 - Step 2** Select the *Name* (active text link) of the switch that you would like to test.
 - Step 3** Click the **Test** button.
-

The switch is tested and the results displayed on screen.

This section also covers:

- [Transit/Transit Server Management on page 318](#)
- [Transit/Voicemail Server Management on page 319](#)
- [Transit/Gatekeeper Management on page 320](#)
- [Transit/IPPBX Server Management on page 321](#)

PGW Server Management

This section covers: Adding, viewing and modifying PGW servers, PGW Server tools and Export.

Add a PGW Server

A PGW Server is a device that is configured by the system as Customers, Locations and Phones lines are added to the IPT environment. The system uses SSH to connect to the PGW to perform configuration changes, however, Telnet is possible if required.

To add a PGW Server:

Procedure

- Step 1** Browse to the relevant sub-menu under the *Network* menu.

- Step 2** Click the **Add** button.
- Step 3** If asked to specify what type of Server you would like to add, click the **Add** button adjacent to the Server type that you would like to add. Alternatively, skip to Step 4.
- Step 4** Complete all of the required fields and click the **Add** button.

The PGW Server is added to the system.

The following fields are available when adding a PGW Server:

Note: Depending on the configuration of your system, some of these fields may not be available.

Attribute	Description
Enter PGW Details	
Name	The name of the PGW, where a PGW may be a single server or dual server deployment. Do not use the & sign in this field in version 3.0.8. This is a mandatory field.
Description	A short description of the PGW.
Software Version	This defines the software version running, and must be set correctly to ensure correct operation. Available options are; PGW : 9.6.1, PGW : 9.7.3, PGW : 9.8, and PGW : 9.9. This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address to use for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring Active?	Select this checkbox if you would like the server to activate Network Monitoring. Note: Depending on network loads, selecting this option may impact on the performance of the server.
Country	Defines the country that the PGW is located in. This is a mandatory field.
Call Processor Id	This Id is used for internal call routing and may either be selected by the administrator or if AUTO is selected, the system will automatically allocate the ID. This is a mandatory field.
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	Select this option if you would like all configuration sessions with the server to be encrypted. Note While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.
Main PGW Server Details	
Note: The following are repeated if a Backup PGW server is used.	
Host Name	This is the DNS host name of the server. This is a mandatory field
Primary IP Address	A PGW may have either one or two network interfaces with an IP Address. This is the Primary IP Address and is the interface that the system will initially use to connect to the PGW. This is a mandatory field.

Attribute	Description
Secondary IP Address	This is the Secondary IP Address and is the interface that the system will use if a connection is not possible via the primary interface.
Config User Id	The PGW server login user id required to configure the PGW.
Config Password	The PGW login password, required to configure the PGW. This is a mandatory field.
Config Prompt	The PGW server prompt displayed when logged using the Config user name. This value is only used if telnet is used to configure the PGW. This is a mandatory field.
MML Command	The system configures the PGW using PGW mml commands. This attribute defines the command used to start an mml session. The default value is mml -s12. This is a mandatory field.
FTP Path	Defines the location on the PGW server to which the system transfers the PGW config files. This is a mandatory field.

View and Modify a PGW Server

From the View and Modify a PGW Server page, the following tools are accessible:

Tool/Task	Accessed Via	Description
HSI Management	Click the HSI Management button.	For more information, see the HSI Management on page 312 help topic.
Load	Click the Load button.	The server is loaded immediately using the specified IOS scripts. Important: No confirmation is requested during this operation.
Test	Click the Test button.	A test of the server occurs immediately and the results of the test are displayed.
Delete	Click the Delete button.	This delete the server from your system. Important: Depending on the configuration of your system, confirmation may be requested prior to deleting a server.
Modify	Make the required changes and click the Modify button.	For more information, see View and Modify a Cisco 36xx Gatekeeper on page 77 .
Prepare for Local Gateway	Click the Prepare for Local Gateway button.	This is used to prepare your PGW for a Local Gateway Role. Important: No Confirmation is requested, this command executes immediately.

Procedure

Modifying a PGW Server

To modify a PGW Server:

- Step 1** Browse to the relevant sub-menu under the *Network* menu.
- Step 2** Select the *Name* (active text link) of the PGW Server that you would like to modify.

Step 3 Modify the required fields and click the **Modify** button.

The PGW Server is modified within the system.

The following fields are available when modifying a PGW Server:

Note

Depending on the configuration of your system, some of these fields may not be available

Attribute	Description
Enter PGW Details	
Name	The name of the PGW, where a PGW may be a single server or dual server deployment. Note The & sign must not be used in this field in version 3.0.8.
Description	A short description of the PGW.
Software Version	This defines the software version running, and must be set correctly to ensure correct operation. Available options are; PGW : 9.6.1, PGW : 9.7.3, PGW : 9.8 and PGW : 9.9.
Service Status	Select from the drop-down list the status of the server.
MCL Limit - Fail Transactions If ...	Select from the drop-down list the conditions under which transactions will fail.
Manual Configuration Mode? (Use for Un-Managed Clusters)	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address to use for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring Active?	Select this checkbox if you would like the server to activate Network Monitoring. Note Depending on network loads, selecting this option may impact on the performance of the server.
Call Processor Id	This Id is used for internal call routing and may either be selected by the administrator or if AUTO is selected, the system will automatically allocate the ID.
Country	Defines the country that the PGW is located in.
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?>	Select this option if you would like all configuration sessions with the server to be encrypted. Note: While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.
Main PGW Server Details	
Note: The following are repeated if a Backup PGW server is used.	
Host Name	This is the DNS host name of the server.

Attribute	Description
<i>Primary IP Address</i>	A PGW may have either one or two network interfaces with an IP Address. This is the Primary IP Address and is the interface that the system will initially use to connect to the PGW. This is a mandatory field.
<i>Secondary IP Address</i>	This is the Secondary IP Address and is the interface that the system will use if a connection is not possible via the primary interface.
<i>Config User name</i>	The PGW server login user name required to configure the PGW.
<i>Config Password</i>	The PGW login password, required to configure the PGW.
<i>Config Prompt</i>	The PGW server prompt displayed when logged using the Config user name. This value is only used if telnet is used to configure the PGW.
<i>MML Command</i>	The system configures the PGW using PGW mml commands. This attribute defines the command used to start an mml session. The default value is mml -s12.
<i>FTP Path</i>	Defines the location on the PGW server to which the system transfers the PGW config files.

PGW Server Tools

PGW Server Tools enable administrators to perform advanced operations on PGW Servers. For more information on available tools, please consult the relevant Feature Guide.

Selecting the Server Type to Add

Depending on the function of the server being added, you may be asked to specify the type of server that you would like to add.

To select the relevant server type, click the **Add** button adjacent to the server type that you would like to add.

The Add Server dialogue appropriate to the server type that you selected is displayed.

Note

Depending on how your system has been configured, and the primary role of the server being added, the list of available servers may differ.

The following server types are available:

Server Type	Description
CCM	The Cisco Call Manager, one of Cisco's foundation Unified communication offerings.
SME	A Cisco Unified Session Manager Edition (Cisco SME) is a transit switch used to aggregate multiple unified communications systems, referred to as leaf systems.
Cisco36xx	A Cisco 36xx Series Router.
CiscoEmergencyResponder	Cisco Emergency Responder ensures that the Cisco Unified Communications Manager (Unified CM) sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.
CiscoSRST	Cisco Secure Survivable Remote Site Telephony. A disaster mitigation technology.

Server Type	Description
Cisco Unity Connection	Cisco Unity Connection provides integrated messaging to assist users manage communications using their phone, PC or both.
IPUnity	IP Unity is a leader in carrier-grade media servers, application servers and real-time multimedia applications for IP and TDM networks.
WebEx	WebEx conference servers from Cisco are hosted servers to which end users can connect via the system's user interface.
ISC	The Cisco IP Solution Center (ISC). A security management solution from Cisco.
Netwise	A Netwise CMG Telephony Server.
PGW Cisco Transit switch	The Cisco PGW (Protocol Gateway) is a multi-protocol, carrier-grade soft-switch designed to support media gateway control functions and interworking in next-generation networks (NGNs).
PGW_TimesTen	The Cisco PGW (Protocol Gateway) multi-protocol, carrier-grade soft-switch described above but with TimesTen capability.
Technician Server	A generic form of server. This is a general purpose server product that is capable of assuming multiple roles.
UnmanagedPBX	Unmanaged PBXs are often used as parent components for a location.

PGW Export

PGW Export is used to export the PGW MML and PGW Times Ten scripts to a text file which can then be manually applied to another PGW. This tool can be used after a new set of PGW models are loaded into the system which allows for the latest scripts and variables to be used.

Note

The tool does not provision any hardware but runs in an export mode, similar to manual mode.

Procedure

Activating the Export Functionality

A system level preference, *AllowPGWexport* is used to enable or disable the export tool. To enable or disable the PGW Export functionality:

- Step 1** Browse to *Setup Tools > Global Settings*.
 - Step 2** Select the *AllowPGWexport* preference.
 - Step 3** Apply the preference.
-

PGW Export is enabled/disabled within your system.

Procedure

Exporting MML and Times Ten data

To export PGW data:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the required PGW.

- Step 3** Click the **Export** button.
- Step 4** Select the required values then click the **Export** button.

Two key files are generated, namely *pgw.txt* and *pgwtimes10.txt*. Certain transactions write to the PGW Times Ten file. In this case, the file is split into a number of smaller files as well as a command file after all the transactions have run successfully. The command file can be used to import the Times Ten files once it has been transferred to the new PGW server. The size of the split files can be changed using the *DriverMaxBulkEntries* model entry in the PGW Times Ten model. The split data files and command file are also compressed into a ZIP file (*PGW_Times_Ten.zip*) which can be transferred and unzipped on the PGW.

Note

The location and name of the file cannot be configured within the system.

Procedure

Viewing MML and Times Ten data

To view the exported PGW data:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the required PGW.
- Step 3** Click the **Export** button.

The *Details:-* section of the screen lists all of the available exported data. Use the *View Files* and *List Files* hyperlinks to view the required data.

HSI Management

To manage your P23 signaling interfaces, follow the steps below.

Procedure

Viewing a P23 Signaling Interface

To view P23 signaling interfaces:

- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that you would like to view the HSI interfaces for.
- Step 3** Click the **HSI Management** button.

A list of the current HSI interfaces is displayed.

Procedure

Adding a P23 Signaling Interface

To add a P23 signaling interfaces:

-
- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that you would like to add a HSI interface to.
- Step 3** Click the **HSI Management** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields and click the **Add** button.
-

The HSI interface is added to the system.

The following fields are available when adding a HSI interface:

Field	Description
Host Name	The host name of the HSI interface. This is a mandatory field.
Description	A short description of the interface.
IP Address	The IP address of the interface. This is a mandatory field.
Config User Name	The user name to be used when configuring the interface.
Config Password	The password to be used when configuring the interface.
Config Prompt	The symbol to be used as the config prompt. This is a mandatory field.
MML Command	The command that will be used for MML. This is a mandatory field.
Software Version	The version of software that will be used by the interface. For example, "HSI : 4.2". This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that will be used for manual activation of the server. This field is mandatory if the Manual Configuration Mode? option has been selected.
Network Monitoring active?	Select this checkbox if you would like to activate Network Monitoring. Note Depending on the configuration of your network, enabling this option may impact on the performance off your network.

Procedure

Deleting a P23 Signaling Interface

To delete a P23 signaling interfaces:

- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that you would like to delete the HSI interface from.
- Step 3** Click the **HSI Management** button.
- Step 4** Select the *Name* (active text link) of the HSI interface that you would like to delete.
- Step 5** Click the **Delete** button.

After confirming the operation, the HSI interface is deleted from the system.

Procedure

Modifying a P23 Signaling Interface

To Modify a P23 signaling interface:

- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that has the HSI interface that you would like to modify.
- Step 3** Click the **HSI Management** button.
- Step 4** Select the *Name* (active text link) of the HSI interface that you would like to modify.
- Step 5** Make the required changes and click the **Modify** button.

After confirming the operation, the HSI interface is updated in the system.

Add a HSI Interface

Procedure

Adding a H323 Signaling Interface

To add a H323 signaling interface:

- Step 1** Browse to *Transit > Network*.
 - Step 2** Select the *Name* (active text link) of the PGW that you would like to add a HSI interface to.
 - Step 3** Click the **HSI Management** button.
 - Step 4** Click the **Add** button.
 - Step 5** Complete the required fields and click the **Add** button.
-

The HSI interface is added to the system.

The following fields are available when adding a HSI interface:

Field	Description
Host Name>	The host name of the HSI interface. This is a mandatory field.
Description	A short description of the interface.
IP Address	The IP address of the interface. This is a mandatory field.
Config User Name	The user name to be used when configuring the interface.
Config Password	The password to be used when configuring the interface.
Config Prompt	The symbol to be used as the config prompt. This is a mandatory field.
MML Command	The command that will be used for MML. This is a mandatory field.
Software Version	The version of software that will be used by the interface. For example, "HSI : 4.2". This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.

Field	Description
Email address for Manual activation	The email address that will be used for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	Select this checkbox if you would like to activate Network Monitoring. Note Depending on the configuration of your network, enabling this option may impact negatively on the performance of your network.

Manage H.323 Signaling Interface (HSI)

H.323 Signaling Interfaces are managed via the *Manage H.323 Signaling Interface* screen.

Procedure

Accessing the Manage H.323 Signaling Interface screen

To access the *Manage H.323 Signaling Interface* screen:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *Host Name* (active text link) that you would like to modify.
- Step 3** Select the *Gateway Name* (active text link) that you would like to modify.
- Step 4** Select the *Transit Switch Name* (active text link) that you would like to modify.
- Step 5** Click the **HSI Manage** button.
- Step 6** Select the *HSI Name* (active text link) of the HSI that you would like to modify.

The following fields are available on the *Manage H.323 Signaling Interface* screen:

Field	Description	Notes
Host Name	The host of the HSI.	This field is provided for information purposes only and cannot be edited via this screen.
Connected PGW	The PGW related to this HSI.	This field is provided for information purposes only and cannot be edited via this screen.
Description	An optional description for the HSI.	-
IP Address	The IP address of the HSI.	This is presented in the typical IP address format, for example, 1.2.3.4.
Config User Name	The configuration user name for the HSI.	This is used to configure the HSI.
Config Password	The configuration password for the HSI.	This is used in conjunction with the above user name.
Config Prompt	The config prompt for the HSI.	-
MML Command	Specify the MML command for the HSI.	-

Field	Description	Notes
Software Version	Select the appropriate software version from the drop-down list.	-
Manual configuration Mode?	Select this checkbox if you would like to use Manual configuration Mode	This option is used mainly for un-managed clusters. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	Specify the email address to be used for manual activation	This field will only accept email addresses in the standard email address format, for example, test@example.com. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	Select this checkbox if you would like to utilize network monitoring.	Note Depending on the configuration of your network, the use of this functionality may lead to degraded network performance.
Date Added	The date the HSI was originally added.	This field is provided for information purposes only and cannot be edited via this page.

Procedure

Delete a HSI

To delete a configuration:

- Step 1** Browse to the *Manage H.323 Signaling Interface* screen using the steps above.
- Step 2** Click the **Delete** button.

After confirming the operation, the interface is removed.

Procedure

Modify a HSI

To modify a configuration:

- Step 1** Browse to the *Manage H.323 Signaling Interface* screen using the steps above.
- Step 2** Modify the required values.
- Step 3** Click the **Modify** button.

The interface is updated within the system.

Manage a H.323 Signaling Interface

Procedure

Modify a P23 Signaling Interface

To Modify a P23 signaling interface:

- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that has the HSI interface that you would like to modify.
- Step 3** Click the **HSI Management** button.
- Step 4** Select the *Name* (active text link) of the HSI interface that you would like to modify.
- Step 5** Make the required changes and click the **Modify** button.

After confirming the operation, the HSI interface is updated in the system.

The following fields are available when modifying the interface:

Note

Depending on the configuration of your system, some of these fields may not be available

Field	Description
Host Name	The host name of the HSI interface. This is a mandatory field.
Description	A short description of the interface.
IP Address	The IP address of the interface. This is a mandatory field.
Config User Name	The user name to be used when configuring the interface.
Config Password	The password to be used when configuring the interface.
Config Prompt	The symbol to be used as the config prompt. This is a mandatory field.
MML Command	The command that will be used for MML. This is a mandatory field.
Software Version	The version of software that will be used by the interface. For example, "HSI : 4.2". This is a mandatory field.
Manual Configuration Mode?	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address for Manual activation	The email address that will be used for manual activation of the server. This field is mandatory if the <i>Manual Configuration Mode?</i> option has been selected.
Network Monitoring active?	Select this checkbox if you would like to activate Network Monitoring. Note Depending on the configuration of your network, enabling this option may impact on the performance off your network.

Procedure**Deleting a P23 Signaling Interfaces**

To delete a P23 signaling interfaces:

- Step 1** Browse to *Transit > Network*.
- Step 2** Select the *Name* (active text link) of the PGW that you would like to delete the HSI interface from.
- Step 3** Click the **HSI Management** button.
- Step 4** Select the *Name* (active text link) of the HSI interface that you would like to delete.
- Step 5** Click the **Delete** button.

After confirming the operation, the HSI interface is deleted from the system.

Transit/Transit Server Management

A Transit Server can be associated with other Transit Servers.

Note

It is necessary to place the EISUP links between these PGWs out-of-service before performing this action. The trunks should be put back in service later.

Procedure

Viewing Associated Transit Servers

To view Transit Servers currently associated to the selected Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit** ==> **Transit** button adjacent to the Transit Server that you would like to disassociate from a Transit Server(s).

A screen is displayed, with two columns, one listing the registered (and available) Transit Servers, and the other displaying the servers current connection status. If the button adjacent to the Transit Server says **Connect**, the Transit Server is available for connection. If the button says **Disconnect**, the Transit Server is already connected.

Procedure

Associating (connecting) a Transit Server to a Transit Server

To associate a Transit Server to a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit** ==> **Transit** button adjacent to the Transit Server that you would like to associate to a Transit Server(s).
- Step 3** Click the **Connect** button adjacent to the Transit Server that you would like to connect.

The Transit Server is associated with the selected Transit Server.

Procedure

Disassociating (disconnecting) a Transit Server from a Transit Server

To disassociate a Transit Server from a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit ==> Transit** button adjacent to the Transit Server that you would like to disassociate from a Transit Server(s).
- Step 3** Click the **Disconnect** button Adjacent to the Transit Server that you would like to disassociate from the Transit Server.

The Transit Server is disassociated from the selected Transit Server.

Transit/Voicemail Server Management

A Transit Server can be associated with a Voicemail Server(s).

Procedure

Viewing associated Transit Servers

To view Transit Servers currently associated to the selected Voicemail Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit ==> Voicemail Server** button adjacent to the Transit Server that you would like to view.

A screen is displayed, with two columns, one listing the registered (and available) Voicemail Servers, and the other displaying the servers current connection status. If the button adjacent to the Voicemail Server says **Connect**, the Voicemail Server is available for connection. If the button says **Disconnect**, the Voicemail Server is already connected.

Procedure

Associating (connecting) a Transit Server to a Voicemail Server

To associate a Transit Server to a Voicemail Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit ==> Voicemail Server** button adjacent to the Transit Server that you would like to associate to a Voicemail Server(s).
- Step 3** Click the **Connect** button adjacent to the Voicemail Server that you would like to connect.

The Transit Server is associated with the selected Voicemail Server.

Procedure

Disassociating (disconnecting) a Transit Server from a Voicemail Server

To disassociate a Transit Server from a Voicemail Server:

- Step 1** Browse to the relevant section under the *Network* menu.

- Step 2** Click the **Transit ==> Voicemail Server** button adjacent to the Transit Server that you would like to disassociate from a Voicemail Server(s).
- Step 3** Click the **Disconnect** button Adjacent to the Voicemail Server that you would like to disassociate from the Transit Server.
-

The Voicemail Server is disassociated from the selected Transit Server.

Transit/Gatekeeper Management

A Transit Server can be associated with a Gatekeeper(s).

Procedure

Viewing Associated Gatekeepers

To view Gatekeepers currently associated to the selected Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit==>Gatekeeper** button adjacent to the Transit Server that you would like to view.

A screen is displayed, with two columns, one listing the registered (and available) Gatekeepers, and the other displaying the Gatekeepers current connection status. If the button adjacent to the Gatekeeper says **Connect**, the Gatekeeper is available for connection. If the button says **Disconnect**, the Gatekeeper is already connected.

Procedure

Associating (connecting) a Transit Server to a Gatekeeper

To associate a Transit Server to a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit==>Gatekeeper** button adjacent to the Transit Server that you would like to associate.
- Step 3** Click the **Connect** button adjacent to the Gatekeeper that you would like to associate with the Transit Server.
-

The Transit Server is associated with the selected Gatekeeper.

Procedure

Disassociating (disconnecting) a Transit Server from a Gatekeeper

To disassociate a Transit Server from a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Transit==>Gatekeeper** button adjacent to the Transit Server that you would like to disassociate from a Gatekeeper(s).

- Step 3** Click the **Disconnect** button adjacent to the Gatekeeper that you would like to disassociate from the Transit Server.

The Transit Server is disassociated from the selected Gatekeeper.

Transit/IPPBX Server Management

A Transit Server can be associated with an IPPBX.

Procedure

Viewing Associated IPPBXs

To view IPPBXs currently associated to the selected Transit Server:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit ==> IPPBX** button adjacent to the SME that you would like to associate/disassociate from a Transit Server(s).

A screen is displayed, with two columns, one listing the registered (and available) IPPBXs, and the other displaying the servers current connection status. If the button adjacent to the IPPBX says **Connect**, the IPPBX is available for connection. If the button says **Disconnect**, the IPPBX is already connected.

Procedure

Associating (connecting) a Transit Server to an IPPBX

To associate a Transit Server to an IPPBX:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit ==> IPPBX** button adjacent to the Transit Server that you would like to associate to an IPPBX.
- Step 3** Click the **Connect** button adjacent to the IPPBX that you would like to connect.

The Transit Server is associated with the selected IPPBX.

Procedure

Disassociating (disconnecting) a Transit Server from an IPPBX

To disassociate a Transit Server from an IPPBX:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit ==> IPPBX** button adjacent to the Transit Server that you would like to disassociate from an IPPBX.
- Step 3** Click the **Disconnect** button adjacent to the Transit Server that you would like to disassociate from an IPPBX.
-

The Transit Server is disassociated from the selected IPPBX

PBX Server Management

For an introduction to PBX Server Management, see: [IP PBX Server on page 95](#).

The following tools are accessible from the Manage PBX Server screen:

Tool/Task	Accessed By	Description
<i>Add a PBX</i>	Clicking the Add button.	For further information, see the Adding a PBX help section: IP PBX Server on page 95 .
<i>Connectivity</i>	Clicking the Connectivity button.	<p>Clicking the Connectivity button displays a page listing the following options. Select the required link (active text link) for more information.</p> <ul style="list-style-type: none"> • IPPBX/Gatekeeper Management on page 323 • IPPBX/Transit Management on page 324 • IPPBX/Emergency Responder Server Management on page 325 • IPPBX/Conference Management on page 326 • IPPBX/Transcoder Management on page 327 • IPPBX/TFTP Management on page 328 • IPPBX/Voicemail Management on page 329 • Managing a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server on page 603 • IPPBX/Third Party SIP Management on page 330 • IPPBX/Location Management on page 331 • PBX to PBX Connection management on page 387 • Call Routing Connections on page 332 • IPPBX/Contact Center Management on page 346
<i>Associated Devices</i>	Clicking the Associated Devices button.	For more information, see the Device Sets on page 347 help topic.

Tool/Task	Accessed By	Description
<i>Tools</i>	Clicking the Tools button.	This opens a page listing the available server tools.

IPPBX/Gatekeeper Management

An IPPBX can be associated with a Gatekeeper(s).

Note

This connection type is typically required for cases where there are gatekeepers working with the PGW.

Procedure

Viewing Associated Gatekeepers

To view Gatekeepers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view
- Step 3** Select the **PBX==>Gatekeeper** button adjacent to the IPPBX that you would like to view

A screen is displayed, with two columns, one lists the registered (and available) Gatekeepers, and the other column displays the Gatekeepers current connection status. If the button adjacent to the Gatekeeper says **Connect**, the Gatekeeper is available for connection. If the button says **Disconnect**, the Gatekeeper is already connected.

Procedure

Associating (connecting) an IPPBX to a Gatekeeper

To associate an IPPBX to a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==>Gatekeeper** button.
- Step 4** Click the **Connect** button adjacent to the Gatekeeper that you would like to associate with the IPPBX.

The IPPBX is associated with the selected Gatekeeper.

Procedure

Disassociating (disconnecting) an IPPBX from a Gatekeeper

To disassociate an IPPBX from a Gatekeeper:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.

- Step 3** Click the **PBX==>Gatekeeper** button.
- Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Gatekeeper(s).
- The IPPBX is disassociated from the selected Gatekeeper.
-

IPPBX/Transit Management

An IPPBX can be associated with a Transit Server(s).

Note

This connection type is typically required for cases where PGW needs to connect to a transit switch.

Procedure

Viewing associated Transit Servers

To view Transit Servers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==>Transit** button adjacent to the IPPBX that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) Transit Servers, and the other column displays the Transit Servers current connection status. If the button adjacent to the Transit Server says **Connect**, the Transit Server is available for connection. If the button says **Disconnect**, the Transit Server is already connected.

Procedure

Associating (connecting) an IPPBX to a Transit Server

To associate a IPPBX to a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==>Transit** button.
- Step 4** Click the **Connect** button Adjacent to the Transit Server that you would like to associate with the IPPBX.
-

The IPPBX is associated with the selected Transit Server.

Procedure

Disassociating (disconnecting) an IPPBX from a Transit Server

To disassociate a IPPBX from a Transit Server:

-
- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Click the **PBX==>Transit** button.
 - Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Transit Server(s).
-

The IPPBX is disassociated from the selected Transit Server.

IPPBX/Emergency Responder Server Management

An IPPBX can be associated with an Emergency Responder Server(s).

Note

This connection type is typically used to enable emergency calls (911). When used, emergency calls are routed via the CER. This is not required to enable emergency dialing, since this can be achieved by conventional LBO call routing.

Procedure

Viewing Associated Emergency Responder Servers

To view Emergency Responder Servers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==> Emergency Responder** button adjacent to the IPPBX that you would like to view.

A screen is displayed with two columns, one lists the registered (and available) Emergency Responder Servers, and the other column displays the Emergency Responder Servers current connection status. If the button adjacent to the Emergency Responder Server says **Connect**, the Emergency Responder Server is available for connection. If the button says **Disconnect**, the Emergency Responder Server is already connected.

Procedure

Associating (connecting) an IPPBX to an Emergency Responder Server

To associate a IPPBX to a Emergency Responder Server:

- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Click the **PBX==> Emergency Responder** button.
 - Step 4** Click the **Connect** button Adjacent to the Emergency Responder Server that you would like to associate with the IPPBX.
-

The IPPBX is associated with the selected Emergency Responder Server.

Procedure

Disassociating (disconnecting) an IPPBX from an Emergency Responder Server

To disassociate a IPPBX from a Emergency Responder Server:

- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Click the **PBX==> Emergency Responder** button.
 - Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Emergency Responder Server(s).
-

The IPPBX is disassociated from the selected Emergency Responder Server.

IPPBX/Conference Management

A IPPBX Server can be associated with a Conference Management Server(s).

Note

This connection type is typically used when running software conferencing on the Unified CM, or when using Webex.

Procedure

Viewing associated Conference Management Servers

To view Conference Management Servers currently associated to the selected IPPBX Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX Server that you would like to view.
- Step 3** Click the **PBX==>Conference** button adjacent to the IPPBX Server that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) Conference Management Servers, and the other column displays the Conference Management Servers current connection status. If the button adjacent to the Conference Management Server says **Connect**, the Conference Management Server is available for connection. If the button says **Disconnect**, the Conference Management Server is already connected.

Procedure

Associating (connecting) a IPPBX Server to a Conference Management Server

To associate a IPPBX Server to a Conference Management Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX Server that you would like to modify.
- Step 3** Click the **PBX==>Conference** button.
- Step 4** Click the **Connect** button Adjacent to the Conference Management Server that you would like to associate with the IPPBX Server.

The IPPBX Server is associated with the selected Conference Management Server.

Procedure

Disassociating (disconnecting) a IPPBX Server from a Conference Management Server

To disassociate a IPPBX Server from a Conference Management Server:

- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX Server that you would like to modify.
 - Step 3** Click the **PBX==>Conference** button.
 - Step 4** Click the **Disconnect** button adjacent to the IPPBX Server that you would like to disassociate from a Conference Management Server(s).
-

The IPPBX Server is disassociated from the selected Conference Management Server.

IPPBX/Transcoder Management

An IPPBX can be associated with a Transcoder Server(s).

Note

This connection type is typically used for third party transcoders, but it not required when using a Unified CM transcoder, since this is supported via IOS devices (HMR role).

Procedure

Viewing associated Transcoder Servers

To view Transcoder Servers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==>Transcoder** button adjacent to the IPPBX that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) Transcoder Servers, and the other column displays the Transcoder Servers current connection status. If the button adjacent to the Transcoder Server says **Connect**, the Transcoder Server is available for connection. If the button says **Disconnect**, the Transcoder Server is already connected.

Procedure

Associating (connecting) an IPPBX to a Transcoder Server

To associate a IPPBX to a Transcoder Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.

- Step 3** Click the **PBX==> Transcoder** button.
- Step 4** Click the **Connect** button Adjacent to the Transcoder Server that you would like to associate with the IPPBX.

The IPPBX is associated with the selected Transcoder Server.

Procedure

Disassociating (disconnecting) an IPPBX from a Transcoder Server

To disassociate a IPPBX from a Transcoder Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==> Transcoder** button.
- Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Transcoder Server(s).

The IPPBX is disassociated from the selected Transcoder Server.

IPPBX/TFTP Management

An IPPBX can be associated with a TFTP Server(s).

Note

This connection type is typically used to connect to third party TFTP servers.
The TFTP role is supported natively on Unified CM.

Procedure

Viewing associated TFTP Servers

To view TFTP Servers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==>TFTP** button adjacent to the IPPBX that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) TFTP Servers, and the other column displays the TFTP Servers current connection status. If the button adjacent to the TFTP Server says **Connect**, the TFTP Server is available for connection. If the button says **Disconnect**, the TFTP Server is already connected.

Procedure

Associating (connecting) an IPPBX to a TFTP Server

To associate a IPPBX to a TFTP Server:

-
- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Click the **PBX==>TFTP** button.
 - Step 4** Click the **Connect** button Adjacent to the TFTP Server that you would like to associate with the IPPBX.
-

The IPPBX is associated with the selected TFTP Server.

Procedure

Disassociating (disconnecting) an IPPBX from a TFTP Server

To disassociate a IPPBX from a TFTP Server:

- Step 1** Browse to the relevant section under the *Network* menu.
 - Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
 - Step 3** Click the **PBX==>TFTP** button.
 - Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a TFTP Server(s).
-

The IPPBX is disassociated from the selected TFTP Server.

IPPBX/Voicemail Management

An IPPBX can be associated with a Voicemail Server(s).

Note

This connection type is typically used to connect to one of the following voicemail servers; Unity or Unity Connection

Procedure

Viewing associated Voicemail Servers

To view Voicemail Servers currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==>VM Server** button adjacent to the IPPBX that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) Voicemail Servers, and the other column displays the Voicemail Servers current connection status. If the button adjacent to the Voicemail Server says **Connect**, the Voicemail Server is available for connection. If the button says **Disconnect**, the Voicemail Server is already connected.

Procedure

Associating (connecting) an IPPBX to a Voicemail Server

To associate a IPPBX to a Voicemail Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==>VM Server** button.
- Step 4** Click the **Connect** button Adjacent to the Voicemail Server that you would like to associate with the IPPBX.

The IPPBX is associated with the selected Voicemail Server.

Procedure

Disassociating (disconnecting) an IPPBX from a Voicemail Server

To disassociate a IPPBX from a Voicemail Server:

- Step 1** Browse to the relevant section under the *Network* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==>VM Server** button.
- Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Voicemail Server(s).

The IPPBX is disassociated from the selected Voicemail Server.

IPPBX/Third Party SIP Management

An IPPBX can be associated with a Third Party SIP.

Note

This connection type is typically used to connect to a SIP Application Server (only UC Central is currently supported). These servers can be added to CUCDM via the Network > SIP Application Servers menu. See under UC Central in the Deployment Guide for more details.

Procedure

Viewing associated Third Party SIPs

To view Third Party SIPs currently associated to the selected IPPBX:

- Step 1** Browse to the *Network > Third Party SIP* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Click the **PBX==> Third Party SIP** button.

A screen is displayed, with two columns, one lists the registered (and available) Third Party SIP Servers, and the other column displays the Third Party SIP current connection status. If the button

adjacent to the Third Party SIP says **Connect**, the Third Party SIP is available for connection. If the button says **Disconnect**, the Third Party SIP is already connected.

Procedure

Associating (connecting) an IPPBX to a Third Party SIP

To associate an IPPBX to a Third Party SIP:

- Step 1** Browse to the *Network > Third Party SIP* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==> Third Party SIP** button.
- Step 4** Click the **Connect** button Adjacent to the Third Party SIP that you would like to associate with the IPPBX.

The IPPBX is associated with the selected Third Party SIP.

Procedure

Disassociating (disconnecting) an IPPBX from a Third Party SIP

To disassociate an IPPBX from a Third Party SIP:

- Step 1** Browse to the *Network > Third Party SIP* menu.
- Step 2** Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.
- Step 3** Click the **PBX==> Third Party SIP** button.
- Step 4** Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Third Party SIP.

The IPPBX is disassociated from the selected Third Party SIP.

IPPBX/Location Management

An IPPBX can be associated with a Location(s).

Note

This connection type is typically required for Unified CM when adding items such as regions, locations, codecs, dialplan elements, location non ER, location ER, SNR patterns, default device pools, and feature configuration templates, or for PGW.

Procedure

Viewing associated Locations

To view Locations currently associated to the selected IPPBX:

- Step 1** Browse to the relevant section under the *Network* menu.

Step 2 Click the **Connectivity** button adjacent to the IPPBX that you would like to view.

Step 3 Click the **PBX==>Location** button adjacent to the IPPBX that you would like to view.

A screen is displayed, with two columns, one lists the registered (and available) Locations, and the other column displays the Locations current connection status. If the button adjacent to the Location says **Connect**, the Location is available for connection. If the button says **Disconnect**, the Location is already connected.

Procedure

Associating (connecting) an IPPBX to a Location

To associate a IPPBX to a Location:

Step 1 Browse to the relevant section under the *Network* menu.

Step 2 Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.

Step 3 Click the **PBX==>Location** button.

Step 4 Click the **Connect** button Adjacent to the Location that you would like to associate with the IPPBX.

The IPPBX is associated with the selected Location.

Procedure

Disassociating (disconnecting) an IPPBX from a Location

To disassociate a IPPBX from a Location:

Step 1 Browse to the relevant section under the *Network* menu.

Step 2 Click the **Connectivity** button adjacent to the IPPBX that you would like to modify.

Step 3 Click the **PBX==>Location** button.

Step 4 Click the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Location(s).

The IPPBX is disassociated from the selected Location.

Call Routing Connections

The purpose of this feature is to support connections to (generic) network elements that are not managed by the system itself. This functionality was introduced to system release 8.0 in order to provide the ability to create trunks as well as configure routing via these trunk(s) to generic network elements to facilitate call routing via a trunk. This is achieved by provisioning route groups and route lists to associate with the new trunk, as well as route patterns.

Before this feature was developed the system only allowed you to create and configure connections between network elements managed within the system. In these cases routing to and from the network element is included as part of the configuration. The new generic connection only enables the provisioning of routing from the system to the generic network element, but because the generic element is not managed in the system, routing from that network element must still be manually configured.

Note

- Only SIP Trunks are currently supported.
- SIP trunks, route groups, route lists, and route patterns configured directly in the Cisco Unified Communications Manager (Unified CM) **before** the introduction of this feature **are not affected**. New trunks and call routing required in Unified CM can be added using this feature. Make sure that any network elements added using this feature do not conflict with pre-existing elements configured in Unified CM. To synchronise settings between the Unified CM and the system, you can either add the exact same elements to the system in manual mode, or delete the details in Unified CM and then re-provision them using this feature.

The Call Routing screen enables you to manage all aspects of call routing connections, trunks, route groups, route lists, and/or route patterns.

Note

You must be a Service Provider Administrator, or higher, to access IP PBX features.

The following functionality is accessible from the *Call Routing - Connections/Trunks/Route Groups/Route Lists/Route Patterns* screen:

Function	Accessed By	Description
<i>Managing Connections</i>	Clicking the Connections button.	You can view, add, modify and/or delete connections. Click the relevant button or link (active text link) to add a new connection, modify an existing connection or to delete the selected connection.
<i>Managing Trunks</i>	Clicking the Trunks button.	You can view, add, modify and/or delete trunks. Click the relevant button or link (active text link) to add a new trunk, modify an existing trunk or to delete the selected trunk.
<i>Managing Route Groups</i>	Clicking the Route Groups button.	You can view, add, modify and/or delete route groups. Click the relevant button or link (active text link) to add a new route group, modify an existing route group or to delete the selected route group.
<i>Managing Route Lists</i>	Clicking the Route Lists button.	You can view, add, modify and/or delete route lists. Click the relevant button or link (active text link) to add a new route list, modify an existing route list or to delete the selected route list.

Function	Accessed By	Description
<i>Managing Route Patterns</i>	Clicking the Route Patterns button.	You can view, add, modify and/or delete route patterns. Click the relevant button or link (active text link) to add a new route pattern, modify an existing route pattern or to delete the selected route pattern.

Limitations. Connections, i.e. trunks, route groups, route lists and route patterns are only provisioned on the local Cisco Unified Communications Manager (Unified CM) IPPBX. Additional configuration of the end-point on the other side of the trunk is not automated, and provisioning of these elements still has to be done manually. Supported trunk types include:

- IP Multimedia Subsystem Service Control (ISC) - from Unified CM version 8.6.2
- Call Control Discovery - from Unified CM version 8.0
- Extension Mobility Cross Cluster (EMCC) - from Unified CM version 8.0. Note that when configuring EMCC manually, you can use this functionality to create/manage the EMCC trunk. EMCC trunks created as part of the EMCC feature are not managed here, and EMCC trunks created here, are not automatically presented/used in the EMCC feature.
- Cisco Intercompany Media Engine (IME) - from Unified CM version 8.0

Note

Trunks, route groups, and route lists cannot be deleted if they are contained in an associated lower level element, for example if a trunk is contained in a route group or if a route group is contained in a route list, etc.

Procedure

Deleting a Connection

To delete a connection, trunk, route group, route list or route pattern:

- Step 1** Click the appropriate button to access the relevant screen, for example **Connections**, **Trunks**, **Route Groups**, etc.
- Step 2** Click the **Delete** button adjacent to the relevant connection you wish to delete. The selected connection is deleted from the system.
-

There are various other buttons available on this screen as follows:

Miscellaneous Buttons

- To search for a specific item, select or enter the relevant search criteria on the appropriate screen, and then click the **Search** button.
- To select all the displayed connections, trunks, route groups, route lists, or route patterns, click the **Select All** button on the appropriate screen.
- To deselect the previously selected connections, trunks, route groups, route lists, or route patterns, click the **Select None** button on the appropriate screen.
- To delete multiple connections, trunks, route groups, route lists or route patterns, select the relevant checkboxes on the appropriate screen, and then click the **Delete Selected** button.

Creating (Adding) Connections

Various methods of creating connections are covered.

Using the Connection Wizard

The connection wizard is one method used to create a complete logical connection by configuring route groups and route lists to associate with the new trunk, as well as route patterns. Together, these four connection elements enable call routing via one or more trunks.

Note

You must be a Provider Administrator to access IP PBX features.

The connection wizard provides the following steps:

- Step 1: Add a Connection
- Step 2: Add a Connection Trunk
- Step 3: Add a Connection Route Group
- Step 4: Add a Connection Route List
- Step 5: Add a Connection Route Pattern to utilize route lists and/or trunks

Click the **Next** button at the end of each step to continue with the next step in the process.

You can exit the wizard (if required) at the completion of any of the steps by clicking the **Finish** button. In this instance, only the connection elements configured at the point of exit are provisioned. The process can then be continued manually at a later stage as described under Using the Standalone Methods (**not** by using the connection wizard).

Adding a Connection

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.
- Step 4** Click the **Add Connection** button. The *Add Connection - 1/5: Add a new Connection* screen is displayed.
- Step 5** Enter the required information in the relevant fields (see below):

Field	Description	Remarks
Connection Name	The name of the connection 'parent' for each routing entity in the Connections feature.	This is a mandatory field
Description	Provide a detailed description for the connection.	-
Device Protocol	Select the required device protocol from the drop-down list.	Only the SIP protocol is currently supported.

- Step 6** Click the **Finish** button when complete to add a connection without a trunk, route group, route list or route pattern to the system, or click the **Next** button to continue to add a trunk to the connection.
-

Adding a Connection Trunk

Procedure

On the *Add Connection - 2/5: Add Trunk(s)* screen:

Step 1

Enter the required information in the relevant fields (see below):

Field	Description	Remarks
Device Name	The name of the device being added, that is <i>Trunk</i> .	This is a mandatory field when adding a trunk, but a read-only field when modifying a trunk. Note that spaces are not allowed in the device name.
Description	A brief description for the device being added.	Spaces are not allowed in the device description.
Device Protocol	The IPT transport protocol for this trunk.	Only the SIP protocol is currently supported.
Connection Parent	Select the Connection Name of the parent connection to which this trunk belongs from the drop-down list.	This is a mandatory field, and can be selected from a drop-down list when adding a trunk outside of the wizard.
Trunk Type	Select the relevant trunk type from the drop-down list.	Only two options are available when adding the trunk using the wizard, namely <i>None</i> and <i>IP Multimedia Subsystem Service Control (ISC)</i> . Three additional options are available when adding the trunk outside of the wizard, namely: <i>Call Control Discovery</i> , <i>Extension Mobility Cross Cluster (EMCC)</i> , and <i>Cisco Intercompany Media Engine (IME)</i> . These trunk types do not use any of the subsequent elements in the wizard, such as route groups, route lists and route patterns. Available trunk types depend on the version of the Cisco Unified Communications Manager (Unified CM) to which the trunk is being added.
Trunk Model Type	Select the relevant trunk model type from the drop-down list.	The Trunk Model Type contains/applies settings that are not exposed via the GUI. This allows an administrator user to create a set of model templates containing pre-determined settings to be used by the user in the GUI by selecting one of the 'templates'. Refer to the Call Manager Model Guide / CCM 6.1.x - SIP Trunks workbook for a list of the settings made available via the model.
SIP Profile	Select the required SIP profile from the drop-down list to apply to the connection.	This field is only available when the SIP device protocol is selected (see <i>Device Protocol</i> field above).

Field	Description	Remarks
Normalization Script	Select the required normalization script from the drop-down list to apply to the trunk.	This field is only available when the SIP device protocol is selected (see <i>Device Protocol</i> field above).
Normalization Script Parameters	Used to customize the normalization script. Enter the key value pairs to be used by the script; for example: <code>key=value;</code> <code>key2=value2;</code> <code>key3=value3</code>	This field is only available when the SIP device protocol is selected (see <i>Device Protocol</i> field above).
Run on Every Node	Select this checkbox is you want this trunk to run on every node in the IPPBX cluster.	Only available for trunk type = None (default).
Destination(s)	Enter the required destination(s).	<p>Maximum of 16 destination addresses. Separate each destination with a comma.</p> <p>A port number may be included in the destination address if required (see examples below).</p> <p>Example 1: Destination(s) = 1.1.1.1:5060, 1.1.1.1:5061, 2.2.2.2:5060 - where the same IP is used with different ports;</p> <p>Example 2: Destination(s) = 1.1.1.1 - where the the port defaults to 5060, unless the port is different in the model for the model type selected;</p> <p>Example 3: Destination(s) = test.com (when Destination is SRV = true) - where the port is set to 0 irrespective of whether a port (e.g. test.com:0), is entered or not.</p> <p>Note</p> <p>Destinations are not required for the <i>Call Control Discovery</i>, <i>Extension Mobility Cross Cluster (EMCC)</i>, and <i>Cisco Intercompany Media Engine (IME)</i> trunk types (see <i>Trunk Type</i> field above).</p>

Step 2 Click the **Finish** button when complete to add the trunk to the connection, or click the **Next** button to continue to add a route group to the connection. Alternatively, when a route group and route list is not required, click the **Add Route Pattern** button to proceed to the last step in the wizard.

Adding a Connection Route Group

Procedure

On the *Add Connection - 3/5: Add Route Group(s)* screen:

Step 1 Enter the required information in the relevant fields (see below):

Field	Description	Remarks
Route Group Name	Enter a name for this route group.	This is a mandatory field, and must be a unique name in the system. Any combination of spaces, periods (.), hyphens (-), and underscore characters (_), up to 50 characters, can be entered as a route group name.
Distribution Algorithm	Define the way in which calls are distributed between the associated trunks by selecting the required option from the drop-down list.	Options include: <ul style="list-style-type: none"> • Circular - Cisco Unified Communications Manager (Unified CM) distributes a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which Unified CM most recently extended a call. If the nth member is the last member of a route group, Unified CM distributes a call starting from the top of the route group. • Top Down - Unified CM distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member.
Connection Parent	Select the Connection entity to which this trunk belongs from the drop-down list if applicable.	This is a mandatory field, and can be selected when adding a Route Group outside of the wizard.

Field	Description	Remarks
Associated Trunks	Add or remove trunks to associate to this route group by selecting the relevant trunk(s) in the <i>Available</i> area of the screen and then clicking the Add>> button, or by selecting the relevant trunks in the <i>Selected</i> area of the screen and then clicking the <<Remove button. Use the <i>Select All</i> link (active text link) to select multiple trunks as required.	<p>The trunks displayed in both the <i>Available</i> and <i>Selected</i> areas of the screen are of the same connection parent.</p> <p>To change the order of the trunks in the <i>Selected</i> area of the screen, select the appropriate trunk, and then click the Move Up or Move Down button as required.</p> <p>Note</p> <p>The trunk order is important as it is used during trunk lookups.</p> <p>Note</p> <p>Trunks associated directly to a route pattern are not displayed. <i>Call Control Discovery</i>, <i>Extension Mobility Cross Cluster (EMCC)</i>, and <i>Cisco Intercompany Media Engine (IME)</i> trunk types are also not displayed as they cannot be associated with a Route Group.</p>

- Step 2** Click the **Finish** button when complete to add the trunk and route group to the connection, or click the **Next** button to add a route list to the route group.

Adding a Connection Route List

Procedure

On the *Add Connection - 4/5: Add a Route List(s)* screen:

- Step 1** Enter the required information in the relevant fields (see below):

Field	Description	Remarks
Route List Name	Enter a name for this route list.	This is a mandatory field, and must be a unique name in the system. Any combination of spaces, periods (.), hyphens (-), and underscore characters (_), up to 50 characters, can be entered as a route list name.
Run on Every Node	Select this checkbox if you want all Unified CM server/s (node/s) in the cluster to be used for call routing.	If this checkbox is selected, the selection in the <i>Call Manager Group</i> (see below) list is ignored.

Field	Description	Remarks
Call Manager Group	Select a specific Unified CM group from the <i>Call Manager Group</i> drop-down list if you want the Unified CM server/s (node/s) in the selected group only to be used for call routing. Note that <i>Default</i> (if present) is merely the Unified CM group created upon initial configuration of the Unified CM cluster.	This field is ignored if the <i>Run on Every Node</i> checkbox is selected (see field above).
Connection Parent	Select the Connection entity to which this route list belongs from the drop-down list (if applicable).	This is a mandatory field and can be specified when adding a Route List outside of the wizard.
Associated Route Groups	Add or remove route groups to associate to this route list by selecting the relevant route group(s) in the <i>Available</i> area of the screen and then clicking the Add>> button, or by selecting the relevant route group(s) in the <i>Selected</i> area of the screen, and then clicking the <<Remove button. Use the <i>Select All</i> link (active text link) to select multiple route groups as required.	<p>A Route list contains Route Groups that are associated to the Route List in a specific order. This order determines the search path which will be taken when locating an available Trunk contained in the Route Groups. When placing a call, the Route List associated with the Route Pattern that is matched becomes the map of available paths for the call. The Route Groups in the Route List are checked in order for an available path i.e. a trunk that is up and has available capacity.</p> <p>The route groups displayed in both the <i>Available</i> and <i>Selected</i> areas of the screen are of the same connection parent.</p> <p>The list of available route groups include the option 'Standard_Local_Route_Group'. This route group will be available for all routegroup-routelist associations on Unified CM.</p> <p>To change the order of the route group in the <i>Selected</i> area of the screen, select the appropriate route group, and then click the Move Left or Move Right button as required.</p> <p>Note</p> <p>The route group order is important in that it is used during route group lookups.</p>

Step 2 Enter each selected Route Group's Called Party Transformations and Calling Party Transformations details.

Each Route Group-Route List association allows for digit manipulation of called and calling numbers, to provide the flexibility of changing number formats when a particular Route Group is used e.g. one Route Group may be a PSTN route that requires the called and calling numbers to be changed from the internal numbering scheme to PSTN format.

The available fields for Called Party Transformations are:

Field	Description	Remarks
Discard Digits	Select from the drop-down list the Discard Digits to apply to the Route Group - Route List mapping.	
Called Party Transformation Mask	Enter the Called Party Transformation Mask to apply to the Route Group - Route List mapping.	
Prefix Digits (Outgoing Calls)	Enter the Prefix Digits (Outgoing Calls) to apply to the Route Group - Route List mapping.	
Called Party Number Type	Select from the drop-down list the Called Party Number Type to apply to the Route Group - Route List mapping.	
Called Party Number Plan	Select from the drop-down list the Called Party Number Plan to apply to the Route Group - Route List mapping.	

The available fields for Calling Party Transformations are:

Field	Remarks	
Use Calling Party's External Phone Number Mask		
Calling Party Transform Mask		
Prefix Digits (Outgoing Calls)	Enter the Prefix Digits (Outgoing Calls) to apply to the Route Group - Route List mapping.	
Calling Party Number Type	Select from the drop-down list the Calling Party Number Type to apply to the Route Group - Route List mapping.	
Calling Party Number Plan	Select from the drop-down list the Calling Party Number Plan to apply to the Route Group - Route List mapping.	

- Step 3** Click the **Finish** button when complete to add the trunk, route group and route list to the system, or click the **Next** button to continue to add a route pattern to the route list.

Adding a Connection Route Pattern

Procedure

On the *Add Connection - 5/5: Add Route Pattern(s)* screen:

Step 1 Enter the required information in the relevant fields (see below):

Field	Description	Remarks
Route Pattern Name	Enter a name for this route pattern.	This is a mandatory field, and must be a unique name in the system.
Description	Enter a detailed description for the route pattern.	It cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Route Pattern	Enter the route pattern.	This is a mandatory field, and is the actual pattern for the string of digits and digit manipulation rules for routing calls to load on the Cisco Unified Communications Manager (Unified CM). Valid characters for a Route Pattern Rule are; [^ 0 1 2 3 4 5 6 7 8 9 A B C D -] + ? ! X * # + . @ \+.
Partition	Select the required partition from the drop-down list into which this route pattern can be loaded.	This is a mandatory field. It can contain a-z, A-Z and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_).
Connection Parent	Select the Connection entity to which this route pattern belongs from the drop-down list.	This is a mandatory field, and can be specified when adding a route pattern outside of the wizard.
Destination Route List / Trunk	Select the required destination route list or trunk from the drop-down list to associate with this route pattern	-
Route Pattern Model Type	Select the required route pattern model type from the drop-down list.	This determines the model template applied when adding this route pattern. Various additional settings are made available via the model (see the Call Manager Model Guide / CCM 6.1.x - Route Patterns workbook).

Step 2 Click the **Finish** button when complete to add the route pattern to the route list.

Using the Standalone Methods

Procedure

Individual connection elements, i.e. trunks, route groups, route lists and route patterns can be added to an existing connection (typically created in step 1 of the wizard - see [Adding a Connection on page 335](#)) as follows:

- Step 1** Browse to *Network > PBX Devices* .
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.
- Step 4** Click the relevant button to add the required connection element, i.e. **Connections, Trunks, Route Groups, Route Lists** or **Route Patterns**.

- Step 5** Enter the required information in the relevant fields of the associated screen(s). These fields are the same as described in the wizard section above.

Call Routing - Connection Details

This screen enables you to modify all aspects of the selected call routing connection. You can add new, or modify existing trunks, route groups, route lists, and/or route patterns, as well as manage the required associations.

Note: You must be a Service Provider Administrator, or higher, to access IP PBX features.

This screen is divided, from top-to-bottom, into the following sections (if configured):

- **Name** - This displays the name of the selected parent connection.
- **Connection Trunks** - All configured trunks are displayed under the *Name* column. The route group to which they are associated is displayed under the *Route Group Name* column. If a route group name is not displayed adjacent to a trunk name, it means that the trunk is currently not associated to a route group.
- **Route Groups** - All configured route groups are displayed under the *Name* column. The route list to which they are associated is displayed under the *Route List Name* column. If a route list name is not displayed adjacent to a route group name, it means that the route group is currently not associated to a route list.
- **Route Lists** - All configured route lists are displayed under the *Name* column. The connection parent to which they are associated is displayed under the *Connection Parent* column.
- **Route Patterns** - All configured route patterns are displayed under the *Name* column. The destination route, i.e. route list or trunk to which they are associated is displayed under the *Destination Route* column.

Managing Connections (Trunks, Route Groups, Route Lists or Route Patterns)

Add a new connection by clicking the relevant **Add.....** button, for example **Add Trunk** or **Add Route Group** button as required.

Modify an existing connection by clicking the relevant *Name* link (active text link).

Note: Individual connections, namely trunks, route groups, and route lists, cannot be deleted if they are contained in an associated lower level element, for example if a trunk is contained in a route group or if a route group is contained in a route list, and so on.

Delete individual connections, for example trunks, route groups, route lists, if required by clicking the relevant **Delete** button adjacent to the connection you want to delete.

Delete the complete parent connection, including all components, if required by clicking the **Delete Connection and its Components** button.

Additional Buttons

Click the **Return to Connections Search** button at the bottom-right of the screen to return to the *Call Routing - Connections* screen.

Click the **Call Routing Summary** button at the top-right of the screen to see a tree view representation of the selected parent connection.

Adding Trunks, Route Groups, Route Lists, and Route Patterns to an Existing Connection

Procedure

If you have already created a connection, you can add/associate trunks, route groups, route lists and route patterns to the connection as follows:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.
- Step 4** Click the relevant connection parent *Name* link (active text link) to view the required connection elements, i.e. Trunks, Route Groups, Route Lists or Route Patterns to the connection parent. The *Call Routing - Connection Details* screen is displayed.
- Step 5** Click the relevant button to add the required connection element, i.e. **Add Trunk**, **Add Route Group**, **Add Route List** or **Add Route Pattern**.
- Step 6** Enter the required information in the relevant fields of the associated screen. These fields are the same as described in the wizard section above.
- Step 7** Click the appropriate **Finish** button when complete.
-

Call Routing Summary

The *Call Routing Summary* screen enables you to view the selected call routing connection in a tree structure view.

The screen is divided into two main sections, namely:

- Name - This displays the name of the selected connection.
- Object Type - This specifies the type of connection, namely; Connection, Trunk, Route Group, Route List, or Route Pattern

Modifying Connections

Modify an existing connection by clicking the relevant *Name* link (active text link).

Delete the complete connection, including its components, if required by clicking the **Delete Connection and its Components** button.

Click the **Return to Connections Search** button at the bottom-right of the screen to return to the *Call Routing - Connections* screen.

Managing Connections via the GUI

Modifying, deleting and viewing connections are covered.

Modifying a Connection

Caution

Modifying connection elements while operations are in progress may result in disruption to existing operations.

Procedure

Modify a configured connection as follows:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.

-
- Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.
 - Step 4** Select the required parent connection *Name* (active text link) that you want to modify. The *Call Routing - Connection Details* screen is displayed.
 - Step 5** Modify or add additional trunks, route groups, route lists or route patterns by selecting the required *link* (active text link) to modify, or by clicking the required **Add...** button, for example **Add Trunk**, **Add Route Group**, etc.
 - Step 6** Modify or enter the required fields (as described in [Using the Connection Wizard on page 335](#)).
 - Step 7** Click the relevant **Modify**, **Modify and Reset**, or **Finish** button (as appropriate) when complete.
 - Step 8** Remove connection elements from a parent connection if required by clicking **Delete** on the relevant **Modify** screen(s).
-

Deleting a Connection

Note

Trunks, route groups, and route lists cannot be deleted if they are contained in an associated lower level element, for example if a trunk is contained in a route group or if a route group is contained in a route list, etc.

Procedure

Delete a configured connection as follows:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
 - Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.
 - Step 4** Select the required parent connection *Name* (active text link) that you want to modify. The *Call Routing - Connection Details* screen is displayed.
 - Step 5** Click the relevant **Delete** button adjacent to the required connection element (connection parent, trunk, route group, route list, or route pattern to delete that specific connection OR
 - Step 6** Click the **Delete Connection and its Components** button at the bottom-left of the screen to delete the entire connection (parent connection and all associated connections).
 - Step 7** Multiple connections can also be deleted from the *Call Routing - Connections* screen by selecting the checkboxes adjacent to the connection names to delete, and then clicking the **Delete Selected** button. The same delete functionality is available on all the individual connection management pages, for example; trunks, route groups, route lists and route patterns.
-

Viewing a Configured Parent Connection

Procedure

View a configured parent connection as follows:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>Connection Destination** button. The *Call Routing - Connections* screen is displayed.

- Step 4** Select the required parent connection *Name* (active text link) that you want view. The *Call Routing - Connection Details* screen is displayed.
- Step 5** Click the **Call Routing Summary** button to display a 'tree-view' of the selected parent connection. All connection elements associated with the parent connection are displayed under the *Name* column and the type of connection element is displayed under the *Object Type* column.
-

Note

You can modify any connection element displayed on this screen by clicking the required *Name* (active text link). Clicking the **Delete Connection and its Components** button results in the deletion of the entire parent connection (including all associated connection elements).

Managing Generic Trunk Connections via Bulk Loaders and Models

Bulk Loaders

Generic Trunk Connections can be managed via the system's bulk loaders. The following worksheets were added to the *03 - Network* bulk loaders for all dial plans to cater for the generic trunk connections functionality within the system:

- Add CCM Connections
- Add CCM Connection Trunks
- Add CCM Connection Route Groups
- Add CCM Connection Route Lists
- Add CCM Connection Route Patterns

Models

In the 1-Leaf-Cluster- Model sheet for all dial plans, the Trunks and RG-Trunks mappings sheets, were renamed to H323-Trunks and RG-H323 Trunk Maps respectively to differentiate them from the SIP Trunks and RG-SIP Trunk Maps sheets.

The following columns were added to the CCM 6.1.x-SIP Trunks sheet to support ISC Trunks:

- Service
- Parameter Label
- Originating Parameter Value
- Terminating Parameter Value
- URI Routing Instructions

IPPBX/Contact Center Management

An IPPBX can be associated with a Contact Center Server(s).

Note

This connection type is typically required to allow lines to be tagged as agent lines at location admin level, and associating such lines to the JTAPI user.

Procedure

Viewing associated Contact Center Servers

To view Contact Center Servers currently associated to the selected IPPBX:

-
- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the **Connectivity** button adjacent to the IPPBX that you would like to view.
- Step 3** Select the **PBX==>Contact Center Server** button adjacent to the IPPBX that you would like to view.

A screen will be displayed, with two columns, one listing the registered (and available) Contact Center Servers, and the other column will display the Contact Center Servers' current connection status. If the button adjacent to the Contact Center Server says **Connect**, the Contact Center Server is available for connection. If the button says **Disconnect**, the Contact Center Server is already connected.

Procedure

Associating (connecting) an IPPBX to a Contact Center Server

To associate a IPPBX to a Contact Center Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **Connectivity** button adjacent to the IPPBX that you would like to modify
- Step 3** Select the **PBX==>Contact Center Server** button
- Step 4** Select the **Connect** button Adjacent to the Contact Center Server that you would like to associate with the IPPBX.

The IPPBX will now be associated with the selected Contact Center Server.

Procedure

Disassociating (disconnecting) an IPPBX from a Contact Center Server

To disassociate a IPPBX from a Contact Center Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **Connectivity** button adjacent to the IPPBX that you would like to modify
- Step 3** Select the **PBX==>Contact Center Server** button
- Step 4** Select the **Disconnect** button adjacent to the IPPBX that you would like to disassociate from a Contact Center Server(s).

The IPPBX will now be disassociated from the selected Contact Center Server.

Device Sets

Device sets are used to associate servers and other network related hardware devices into logical groups. These groups are called device sets. Device sets can be configured based on location, function etc. From the Device Sets screen you are able to add and delete device sets but not modify device sets.

Note

More than one device must be configured before a Device Set can be created.

Procedure

Add A Device Set

To add a device set:

- Step 1** Browse to the *Network > PBX Devices* menu item. The *Manage PBX Server* screen is displayed.
- Step 2** Click the **Associated Devices** button adjacent to the required PBX Server name. The *Manage Device Set* screen is displayed.
- Step 3** Click the **Add** button. The *Add Device Set* screen is displayed
- Step 4** Complete all of the required fields. The following fields are available when adding a Device Set:

Note

Depending on the configuration of your system, certain fields may not be available.

Field	Description
<i>Set Name</i>	The name of the Device Set being added. This is a mandatory field.
<i>Description</i>	A short description of the device set being added.
<i>Primary Host</i>	The device that acts as the primary host in the Device Set. This field cannot be modified by the user.
<i>Device Type</i>	The device type of the device that acts as the primary host in the Device Set. This field cannot be modified by the user.
<i>Transaction Type</i>	Select the type of transactions that this device manages, options include Add Customer, Add Location, Connect Location to Shared Gateway, Connect Location to Dedicated Gateway, etc.
<i>Available Devices</i>	This section of the screen lists all of the available devices that can be added to the Device Set. Select the checkbox(es) adjacent to the device(s) that you would like to add to the Device Set.

- Step 5** Click the **Submit** button when complete. The Device Set is added to the system.

Procedure

Delete a Device Set

To delete a device set:

- Step 1** Browse to the *Network > PBX Devices* menu item. The *Manage PBX Server* screen is displayed.
- Step 2** Select the *Name* (active text link) of the device set that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the Device Set is deleted from the system.
-

Add a Device Set

Device sets are used to associate servers and other network related hardware devices into logical groups. These groups are called device sets. Device sets can be configured based on location, function etc.

Note: More than one device must be configured before a Device Set can be created.

Procedure

Add a Device Set

To add a device set:

- Step 1** Browse to the relevant menu item, under the *Network* menu.
- Step 2** Select the **Name** (active text link) of the hardware device that you would like to create a device set for.
- Step 3** Click **Associate Device** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required field and click the **Add** button.

The Device Set is added to the system.

The following fields are available when adding a Device Set:

Note: Depending on the configuration of your system, certain fields may not be available.

Field	Description
<i>Set Name</i>	The name of the Device Set being added. This is a mandatory field.
<i>Description</i>	A short description of the device set being added.
<i>Primary Host</i>	The device that acts as the primary host in the Device Set. This field cannot be modified by the user.
<i>Device Type</i>	The device type of the device that act as the primary host in the Device Set. This field cannot be modified by the user.
<i>Transaction Type</i>	Select the type of transactions that this device set manages, options include Add Customer, Add Location, Connect Location to Shared Gateway, Connect Location to Dedicated Gateway, etc.
<i>Available Devices</i>	This section of the screen lists all of the available devices that can be added to the Device Set. Select the check-box(s) adjacent to the device(s) that you would like to add to the Device Set.
<i>The system</i>	Select this checkbox if you would like the device set to be available within the system.

Connecting an Unmanaged Legacy PBX to another PBX

This section covers connectivity from a leaf cluster for TDM Connectivity via an MGCP Gateway as well as IP Connectivity using H323 Trunks and SIP Trunks.

TDM Connectivity via an MGCP Gateway from a Leaf Cluster

Prerequisites:

- An Unmanaged Location, using an unmanaged Hardware Group, is a prerequisite for adding a MGCP Gateway.
- The Hardware Group used by the location must have "Adding Locations - Unmanaged Legacy" selected for the Limit usage of this Hardware Group to: field.

Procedure

- Step 1** Add an IPPBX Connected MGCP Legacy PBX Gateway as follows:
- a Browse to Network > IOS Devices.
 - b Select the **Add** button adjacent IPPBX Connected MGCP Legacy PBX Gateway.

- c** Provide the IOS Device details.

Note

Only Unmanaged Locations will be available for selection from the drop-down list. Therefore, the existence of an Unmanaged Location, using an unmanaged Hardware Group, is a prerequisite for adding this Gateway type.

- d** Select the **Next** button.

- e** Configure the MGCP Gateway Details. Please note the handling of the following fields when configuring MGCP Gateways:

- Select a Cisco Unified Communications Manager from the *Select Device* drop-down list
- Select the relevant Gateway Chassis from the drop-down list
- The Gateway function, Legacy, is pre-selected and other roles cannot be added

For more information on how to add an IOS Device, please see [Adding an IOS Device on page 290](#).

- f** Click the **Next** button.

- g** Configure the relevant module slots for the chassis selected.

Note

For this Gateway type, only E1 and T1 ports are supported; however, all port types will be displayed in the respective drop-downs.

- h** Click the **Finish** button.

Step 2 Configure ports for the gateway as follows:

- a** Browse to *Network > IOS Devices* and select the relevant IOS Device's *host Name* (active text link).
- b** On the next screen, in the Device Roles section, select the Gateway's *Name* (active text link).
- c** On the next screen, in the *Interface Details (Available Interfaces)* section, click the **Gateway Hardware Configuration** button.
- d** On the next screen, click the **port** buttons (buttons are labeled with the port names) to configure.
- e** On the next screen, provide the configuration details for the port.

Note

- For this Gateway type and the type of port selected (T1 or E1) the PRI Protocol Type will have a default value of "PRI ISO QSIG T1" or "PRI ISO QSIG E1".
- ISDN Switch Type is also defaulted to "primary-qsig".

For more information on Port Configuration, see [Configuring Legacy Ports on page 294](#).

Step 3 Allocate the configured ports to a location.

- a** Browse to *Network > IOS Devices*, and then select the relevant IOS Device's *host Name* (active text link).
- b** On the next screen, in the Device Roles section, select the Gateway's *Name* (active text link).

- c On the next screen, in the Service Details (Legacy Interfaces) section, click the **Port Allocation** button.
- d On the next screen, in the Legacy Port Allocation (Unallocated Ports) section, select from the drop-down list the relevant unmanaged location and select from the list the ports to allocate to the location.
- e click the **Allocate** button.

Step 4 Activate the ports at the location level, by following these steps:

- a Browse to Location Administration > Telephony.
- b Select Location Unmanaged Legacy Gateways (active text link).
- c Select the ports to activate for the relevant deactivated Gateway.
- d Click the **Activate** button.
- e On the next screen, a Calling Search Space (CSS) text field is displayed, with a default value populated from the loaded HCS model. Leave this value as the default or change it to the appropriate CSS value.
- f Specify the *Call Agent Order* by selecting a port from the list and then moving its position in the order up or down by selecting the up or down buttons.
- g Click the **Add** button.

Note

When activating the ports, the IPPBX selected at Gateway configuration is provisioned with the Route Lists, Route Groups and Route Patterns configured in the loaded HCS model.

IP Connectivity using H323 Trunks from a Leaf Cluster

Procedure

Connect an unmanaged PBX to a managed PBX using H323 Trunks as follows:

- Step 1** Browse to *Network > PBX Devices* and click the **Connectivity** button associated with the relevant PBX.
- Step 2** On the next screen, click the **PBX => PBX** button.
- Step 3** Select the checkbox adjacent the relevant managed PBX to which the unmanaged PBX should be connected.

Note

Unmanaged PBX's can only be connected to managed PBX's via the GUI.

- Step 4** Click the **Connect H323 trunk** button adjacent the selected PBX to perform the connection.
-

IP Connectivity using SIP Trunks from a Leaf Cluster

Procedure

Connect an unmanaged PBX to a managed PBX using SIP Trunks as follows:

- Step 1** Browse to *Network > PBX Devices* and click the **Connectivity** button associated with the relevant PBX.
- Step 2** On the next screen, click the **PBX => PBX** button.
- Step 3** Select the checkbox adjacent the relevant managed PBX to which the unmanaged PBX should be connected.
- Note**
- Unmanaged PBX's can only be connected to managed PBX's via the GUI.
- Step 4** Click the **Connect SIP trunk** button adjacent the selected PBX to perform the connection.
-

Call Routing

This section outlines how Call Routing can be applied and managed in the system. Call Routing can be configured after provisioning the dialplan for local gateways at the location. Once the dialplan is configured for local gateways at the location, a new section Call Routing Management will be visible within the gateway management module at the Location Administration level.

This section allows call routing types to be configured at the location level which involves configuration to be applied to the Cisco Unified Communications Manager. Once the call routing types have been configured with the local call path at the location level, they will be available for configuration by the local gateway H323 ports activated at the location. This requires configuration to be applied at the gateway itself.

Defining Call Routing Types in the system

Call Routing Types can be defined in the system as service types, having a service category of *gatewaycallrouting* . Call Routing Types can be added via *Setup Tools > Service Types* in the system. A set of call routing types is available by default in the system. The table below lists the call routing types available, by default, in the system.

Service Type Name	Service Type Description
1	National
2	International
3	Emergency
4	Service
5	Mobile
6	FreePhone
7	Premium
8	Low-Cost
9	Local

Associate Call Routing Types to Country

Call Routing Types can be associated with a country to define a set of call routing types supported by that country. To associate call routing types with a country, browse to *Dialplan Tools > Countries* .

The section called, *Supported Gateway Call Routing Types*, is available on the *Add and Manage Country Pages* .

This section lists all of the call routing types available in the system, adjacent to each is a checkbox that enables you to select the call routing types that need to be associated with the

selected country. The *Country Call Type Name* setting is used to define the names of the call routing types within the selected country. By default, the country call type name is populated as the service type description setting for the call routing type.

The call routing type can also be associated with countries using the bulk loaders. The *Add Country Bulk loader* has been updated to update the call routing types for the country. The column name used to associate call routing types to country is *Gateway Call Routing Type 1....n* where max value for n is 100.

Valid formats for this column are:

- <Call Routing Type>: <Country Call Type Name>: Used if a name needs to be provided. For example, if call routing type is 1 and the country call type name is desired to be National, the column will take the value: 1:National.
- <Call Routing Type>: Used if a country call type needs to default to the service type description setting. If the Country Call Type Name needs to default to service type description, the column would take the value: 1

Applying Call Routing at Location Level

After the dialplan is configured for local gateway ports at the location aspects such as call routing can be managed at the location level. The location level gateway configuration page is accessed by browsing to *Location Administration > Telephony > Gateways > Gateway*. The call routing configuration page is accessed by clicking the **Call Routing** button on the *Gateway Index* page.

The first section available on the screen is for *Location Level Call Routing*. This section lists all the call routing types associated with the country of the location and have radio buttons against each to select between central or local call paths. The **Submit** button is used to add the call routing to the location level.

Once the location level call routing has been applied, a **Modify** button is available to modify the location level call routing. If the call routing type is being used at the IOS device port level, the call path for it cannot be modified and the radio buttons for the call paths will be disabled. The location level call routing can be deleted if no local gateway port call routings are applied.

Configuration applied to Cisco Unified Communications Manager

When adding the location level call routing, the route patterns and translation patterns associated with the call routing types that have local call paths are updated. The route list for the route patterns associated with the location and having call routing type having local call path are updated to Local Gateway Route List setting of the route pattern. Similarly, the calling search space for the translation patterns associated with the location, and having local call path, is updated to Local Gateway CSS setting of the translation pattern.

While modifying the location level call routing, the route patterns and translation patterns associated with the call routing types being modified are updated.

The route list for the route patterns associated with the location, and associated with the call routing types for which the call path is modified to central, are updated to route list name setting of the route pattern. Similarly, the calling search space for the translation patterns associated with the location, and associated with the call routing types for which the call path is modified to central, update the CSS name setting of the route pattern.

The route list for the route patterns associated with the location, and having call routing type having local call path, are updated to Local Gateway Route List setting of the route pattern. Similarly, the calling search space for the translation patterns associated with the location, and having local call path, are updated to Local Gateway CSS setting of the translation pattern.

While deleting the location level call routing, the route patterns and translation patterns associated with the call routing types having local call path are updated.

The route list for the route patterns associated with the location, and having call routing type having local call path, are updated to route list name setting of the route pattern. Similarly, the calling search space for the translation patterns associated with the location, and having local call path, are updated to CSS name setting of the translation pattern.

Cisco Unified Communications Manager configuration when adding/updating Translation Patterns and Route Patterns

When adding and/or updating translation patterns and route patterns, if the patterns are associated with call routing type configured to have local call path at the location for which the pattern is being added, the route list for the route pattern is updated to local gateway route list setting and the calling search space of the translation pattern is updated to local gateway CSS setting of the pattern.

Local Gateway Port Call Routing

The *Local Gateway Port Call Routing* section is displayed on the screen once the location level call routing has been applied and H323 ports have been activated at the location. The first setting displayed in this section is *Apply Call Routing Configuration to Trunks*, this has two options available, these are *Once for all the Call Types* and *Once per Call Type*. By default, *Once for all Call Types* is selected. This implies that call routing configuration will be applied to trunks once for all the call types. If *Once per Call Type* is selected, the configuration would be applied per call type per trunk. Once call routing has been applied to the ports, the *Apply Call Routing Configuration to Trunks* setting cannot be modified, and the drop-down menu is disabled.

The section also lists all the H323 ports activated at the location with call routing types configured with local call path against each of them. Checkboxes are displayed against each of the call routing type to select the call routing type for the H323 ports. Once the local gateway port call routing has been applied, **Modify** and **Delete** button are displayed in the section to modify and delete the local gateway port call routing.

Configuration Applied on the Gateway

Configuration applied to the gateway depends on the setting *Apply Call Routing Configuration to Trunks*. The IOS Script name that will be applied is *[Add/Del/Mod]LocalGWPortCallRouting - H323*. Add and Del IOS scripts are applied for the ports for which the call routing has been configured.

While modifying the local gateway port call routing, the *Mod IOS* script is applied for the ports for which call routing has been configured. For the ports for which the call routing has been removed (i.e. not even one call type has been selected) the *Del IOS* script is applied.

The variables available for these scripts are as follows:

- #TRUNKID# - IOS device port id
- #CALLTYPE# - Call Routing Type
- #CALLTYPELIST# - List of the selected call routing type for the trunk
- #SUBCTCOSS# - If the trunk has Local (9) call routing type selected then this is set to ","
- #PORTNUM# - Port Number
- #PREFERENCE# - Device Priority of the Port
- #DCHAN# - dchannel setting of the port
- #PSTNACCESSPREFIX# - externalaccessprefix setting of the location
- #STDACCESSPREFIX# -stdaccessprefix of the country
- #NATCODE# - Local Dialing Area Code of the Port

- #OUTLDNAC# - Local Dialing Area Code of the Port
- #INLDNAC# - Local Dialing Area Code of the Port

Bulk Loader and Model Loader Changes

Changes to the Country Loader and Model loaders are listed here.

Add Country Loader Changes

The *Add Country Bulk loader* has been updated to update the call routing types for the country. The column name used to associate call routing types to the country is *Gateway Call Routing Type 1...n*, where max value for n is 100. The valid format for this column is: *<Call Routing Type: Country Call Type Name>* or just *<Call Routing Type>* if country call type needs to default to the service type description setting. For example, if call routing type is 1 and the country call type name is desired to be National, the column will take the value *1:National*. If the Country Call Type Name needs to default to the service type description, the column would take the value *1*.

Route Patterns Model Loader Changes

Two new optional columns are available called *Gateway Call Routing Type* and *Local Gateway Route List*. *Gateway Call Routing Type* takes in a valid service type value having the service category *gatewaycallrouting*.

Translation Patterns Model Loader Changes

Two new optional columns are available called *Gateway Call Routing Type* and *Local Gateway CSS*. *Gateway Call Routing Type* takes in a valid service type value having service category as *gatewaycallrouting*.

The Survivable Remote Site Telephony (SRST)

The Survivable Remote Site Telephony (SRST) support in the system enables an IPPBX connected to a gateway, to use an SRST device role. The system manages:

- Adding the SRST reference to the Cisco Unified Communications Manager
- Adding device pools to the location using a typical or custom device pool template.
- Providing IOS models to enable IOS configuration

Note

Due to limitations in the Cisco Unified Communications Manager (Unified CM) AXL interface, adding the SRST config in Unified CM is a manual step for Unified CM 4.2 and earlier.

When adding or deleting an SRST role to an IOS Device, system features may need to be applied. These include features such as Emergency Number, Emergency CLI, Associate FNN Range and Forward User DDI.

SRST Role

Adding an SRST Role to an IOS Device

Note

To modify an existing IOS Device SRST role, click the **Configure** button in the *SRST Configuration* area of the *Device Roles* section of the screen.

Procedure

To add an SRST role in an IOS Device:

- Step 1** Browse to *Network > IOS Devices*.
- Step 2** Select the *SRST* checkbox in the *Device Roles* section of the *Add IOS Device* screen.
- Step 3** Click the **Add** button in the *Device Roles* section to add an SRST role to a device. The *IOS Device - SRST Configuration* screen is displayed.
- Step 4** Complete the required fields. The following fields are available in the *SRST Details* section of the screen:
- **SRST Reference Name:** The name of the SRST reference added to Cisco Unified Communications Manager (Unified CM). This is a mandatory field.
 - **Protocol:** Select the required protocol, which is used to select the correct model to run in order to provision the SRST device. This is a mandatory field. Cisco Unified Communications Domain Manager (CUCDM) only supports the SIP and H323 protocols.
 - **IP Address:** The IP Address of the IOS device. This is a mandatory field.
 - **SRST Port Number:** The port for the SRST connection. Used for the SRST reference in Unified CM. This is a mandatory field.
 - **SIP Network/IP Address:** The SIP address or IP address of the SRST device. Used for the SRST reference in Unified CM. If an IP address is used, no NAT support is provided.
 - **SIP Port Number:** Port number used if it is a SIP SRST connection. Used for the SRST reference in Unified CM. This is a mandatory field.
 - **Is Secure?:** Checkbox to indicate secure SRST. Used for the SRST reference in Unified CM.
 - **Max Conferences:** Value to indicate the max number of conferences the SRST device will support. Used to provide a variable for the IOS model for the ccm-fallback config. This is a mandatory field.
 - **Max IP Phones:** Maximum phones supported by the SRST setup. Used to provide a variable for the IOS model for the Unified CM - fallback config. This is a mandatory field.
 - **Allocated IP Phones:** This is a read-only field showing the current number of phones that have been allocated to this SRST instance.
 - **Max Directory Numbers:** Maximum directory numbers supported by the SRST setup. Used to provide a variable for the IOS model for the ccm-fallback config. This is a mandatory field.
 - **Voicemail E.164 Fallback Number:** .
 - **SRST User Locale:** This is a free text field, which allows the administrator to configure the required locale (country code) of the SRST device. This identifies a set of detailed information to support users, including language and font.

The following details need to be provided in the *SRST Device Pool Details* section on the *IOS Device - SRST Configuration* screen:

- **Device Pool Config:** Select the Typical or Custom radio button.
- **Create SRST Device Pool based on Device Pool:** This drop-down list displays all the device pools in the location. When the first SRST role is added to a Gateway in this location, this dropdown defaults to the Location's default device pool. If the administrator leaves this as is, then an SRST device pool is created based on the Location's default device pool (a copy is made, and the new SRST Reference is added.) Otherwise the administrator can choose a different device pool to use as a template for the new SRST device pool. Both "Location" and "SRST" device pools are listed in this drop-down list. Further SRST-device pool associations

can be made via Add/Edit Device Pool at Location Administration -> Telephony -> Device Pools. Select the required device pool from the drop-down list of all device pools at the location.

If the *Custom* radio button was selected then complete the following additional SRST device pool custom fields:

- **Name:** The name of the device pool that you are creating. This is a mandatory field and must be unique.
- **Description:** A descriptive name for the device pool.
- **Device Pool Type:** SRST or Location
- **Device Pool Template:** This is a mandatory field. Select the required device pool template from the drop-down list.
- **Call Manager Group:** Read-only field as specified in the device pool template.
- **Date/Time Group:** Specifies the date and time zone for the device.

Note

Date/time groups deleted in Unified CM are no longer displayed in this drop-down if the *Import/Refresh CCM Items - Date/Time Groups* option has been initiated in CUCDM.

- **Audio Region:** This is a mandatory field. Select the audio region to assign to devices in this device pool. This specifies the voice codec that can be used for calls within a region and between other regions.
- **Supported Streams:** The device pool capacity allocated to the device pool.
- **Local Route Group:** Read-only field. None or from Global Settings as specified in the selected device pool template.
- **AAR CSS:** Specifies the calling search space for the device to use when performing automated alternate routing (AAR). Read-only field. None or from Global Settings as specified in the selected device pool template.
- **AAR Group:** Specifies the AAR group for the device. The AAR group provides the prefix digits that are used to route calls that are blocked due to insufficient bandwidth. Read-only field. None or from Global Settings as specified in the selected device pool template. An AAR group setting of None specifies that no attempt to reroute blocked calls will occur.
- **Calling Party Transformation CSS:** Read-only field. None or from Global Settings as specified in the selected device pool template.
- **Called Party Transformation CSS:** Read-only field. None or from Global Settings as specified in the selected device pool template.

- Step 5** Click the **Add** button when complete to save the changes and add the SRST role to the IOS device (or the **Modify** button if modifying an existing SRST role).

Once the *SRST* configuration is saved, the *SRST* reference is available to the location's device pools.

Note

When the *SRST* is added, the *AddSRST* transaction is run in the system. This updates the system with the details and also calls the following drivers:

Driver_IPPBX

This will setup the PBX connected to the Gateway with the *SRST* reference and a device pool for the location with the *SRST* reference.

Note

This configuration is not added for Cisco Unified Communications Manager (Unified CM) 4.2 due to API limitations (the transaction in the system will complete successfully with a message that the automated config isn't supported). This needs to be done manually via the Unified CM admin interface prior to setting up the config in the system using the names as indicated above.

Driver_PSTN

This calls the IOS models to determine what configuration to apply to the IOS device.

Modifying an *SRST* Role

All of the *SRST* configuration can be updated (modified). This applies the updated configuration to the PBX and the IOS Device. When the *SRST* configuration is modified, the *ModSRST* transaction is run in the system.

This updates the system with the details and also calls the following drivers:

Driver_IPPBX

This updates the *SRST* reference with any modified settings.

Note

For Cisco Unified Communications Manager (Unified CM) 4.2, the configuration changes in the system are not reflected in Unified CM. This must be done manually similarly to the add process.

Driver_PSTN

This calls the IOS models to determine what configuration to apply to the IOS device.

Delete an *SRST* Role

The *SRST* role and config can be deleted as required **if it is not in use by any phones in the location**. When this is done, the *DelSRST* transaction is run in the system which updates the system and calls the following drivers:

Driver_IPPBX

This deletes the *SRST* reference.

Driver_PSTN

This calls the IOS models to determine what configuration to apply to the IOS device.

Note

All phones in a location need to be removed from the *SRST device pool* before this delete can happen. This can be done by disabling *SRST* for all phones via

phone management. The SRST role can not be deleted if the SRST reference is used by any device pool at the location.

Assigning *SRST* to a Phone

The availability of the *SRST* feature for a phone is controlled via the feature group. *SRST* functionality must be enabled for the relevant feature group by selecting the *SRST* checkbox in the *Handset* section on the *Manage Feature Group* screen.

Note

This appears in the feature group as *SRST Enabled* in earlier versions of the system, this is the same service type. If this setting is enabled in a phone's feature group, *SRST* setting can be enabled/disabled for the phone on the *Phone Management* screen.

The *SRST* checkbox on the *Phone Management* screen is used to enable or disable the *SRST* feature for the phone. If selected, a drop-down list is displayed showing all *SRST* references available at the Location. Select the required *SRST* reference from the drop-down list, for example "TestSRST Ref - IP Phones allocated: [0] - Available: [10]". This drop-down list also indicates the number of IP Phones allocated to the *SRST* reference, as well how many can still be allocated. In the example *SRST* reference, the number of IP phones allocated to the *SRST* reference is 0, and the amount of IP phones that can still use the *SRST* reference is 10.

To enable *SRST* for a phone, select the *SRST* checkbox on the relevant phone's *Phone Management* screen, and then select the required *SRST* reference from the drop-down. The *SRST* reference selected determines the *SRST* device pool used for the phone during the modify transaction.

If the location does not have a *SRST* reference, then when the *SRST* checkbox is selected for the phone, the drop-down indicates that no *SRST* references are configured. If the modify is submitted like this (*SRST* checked, but no references) then the *SRST* setting is cleared and the phone remains in the normal location device pool.

Disabling the *SRST* checkbox and modifying, results in the phone returning to the usual location device pool, and *SRST* resources freeing-up on the *SRST* reference.

Note

The number appended to the end of the *SRST device pool* may not be the same as the location device pool as the *SRST* device pool uses the gateway-id instead of the location-id. This is due to the fact that a location could have multiple *SRST* references and *SRST* device pools.

NAT for Gateways

This functionality provides the ability to cater for a NAT boundary between the Unified CM and the Gateway device. In this type of environment, the NAT boundary can be one-way or two-way. Two settings on the gateway allow the specification of this behavior:

- **Unified CM to use Gateway IP B** - This causes Unified CMs communicating with this device to use the IP address configured in *IP Address B* on the Gateway. This option allows communication from the Unified CM to the Gateway via a NAT Boundary.
- **Gateway to Use Unified CM IP B** - This Gateway uses the Unified CM IP address configured in the *IP Address B* field on the Unified CM configuration screen. This option allows communication from the Gateway to the Unified CM via a NAT Boundary.

The impact of these settings determines how IP Address settings are configured on the devices.

When configuring an IOS Device and gateway, you can provide a NATed address in *IP Address B* for the gateway device. Also, a NATed address can be provided for each Unified CM server in *IP Address B* when adding it to the cluster.

Note

- The *Gateway to Use Unified CM IP B* option is only valid for Unified CMs. An error message is returned if a Unified CM is not used. Transit switches are not supported by this option.
 - *IP Address B* must be configured for the Unified CM if the *Gateway to Use Unified CM IP B* option is selected.
 - When the *Unified CM to use Gateway IP B* option is selected, an error is returned if the *IP Address B* field on the Gateway is not complete as this is a mandatory field when *Unified CM to use Gateway IP B* is selected.
-

NAT of Gateway Address to Unified CM

If the *Unified CM to use Gateway IP B* setting is selected for the gateway, the *IP Address B* of the gateway is used everywhere the IP address is used for configuration in the Unified CM.

This has the following impact on protocols:

- **H323** - This is used as the device name in the Cisco Unified Communications Manager (Unified CM) and in related transactions which reference the device name, for example *AddLocationLocalGW*.
- **SIP** - This is used to configure the SIP Trunk name and destination in the Unified CM. It is also used for any transactions that reference the trunk name, for example route patterns for the registration of analog devices.

Note

When the *Unified CM to use Gateway IP B* option is selected, an error is returned if the *IP Address B* field is not complete in the Gateway, as this is a mandatory field when *Unified CM to use Gateway IP B* is selected.

NAT of Unified CM Address to Gateway

If the *Gateway to Use Unified CM IP B* setting is selected for the gateway, the *IP Address B* field of the Unified CM is used everywhere the IP Address is used for configuration of the Gateway.

- **SIP** - Any call agent IP Address variables in the various models will be substituted with the Unified CM *IP Address B*.
- **H323** - Any call agent IP Address variables in the various models will be substituted with the Unified CM *IP Address B*.

Guidelines for usage based on specific NAT configuration

The following scenarios outline when to use the various options available.

1. If no NAT boundaries are used between the Gateway and Unified CM, then
 - only *IP Address* needs to be configured on the Unified CM,
 - only *IP Address* needs to be configured on the Gateway,

- the Gateway option *Unified CM to use Gateway IP B* must not be selected (*Unchecked*), and
 - the Gateway option *Gateway to Use Unified CM IP B* must not be selected (*Unchecked*).
2. If communication from the Unified CM to the Gateway passes through a NAT boundary, but **not** from the Gateway to the Unified CM, then
- only *IP Address* on the Unified CM must be specified,
 - the *IP Address B* on the Gateway must be specified,
 - the Gateway option *Unified CM to use Gateway IP B* must be selected (*Checked*), and
 - the Gateway option *Gateway to Use Unified CM IP B* must not be selected (*Unchecked*).
3. If communication from the Unified CM to the Gateway does **not** pass through a NAT boundary, but it does from the Gateway to the Unified CM, then
- the *IP Address B* on the Unified CM must be specified,
 - only *IP Address* on the Gateway must be specified,
 - the Gateway option *Unified CM to use Gateway IP B* must not be selected (*Unchecked*), and
 - the Gateway option *Gateway to Use Unified CM IP B* must be selected (*Checked*).
4. If communication from the Gateway to the Unified CM passes through a NAT boundary, as well as communication from the Gateway to the Unified CM, then
- the *IP Address B* on the Unified CM must be specified,
 - the *IP Address B* on the Gateway must be specified,
 - the Gateway option *Unified CM to use Gateway IP B* must be selected (*Checked*), and
 - the Gateway option *Gateway to Use Unified CM IP B* must be selected (*Checked*).

PGW Export Tool

The PGW export tool is used to export the PGW MML and PGW Times Ten scripts to a text file which can then be manually applied to another PGW. This tool can be used after a new set of PGW models are loaded into the system which allows for the latest scripts and variables to be used.

Note

The tool does not provision any hardware but runs in an export mode, similar to manual mode.

Supported Transactions

Transactions currently supported include:

- InitTransit
- ConnectTransitTransit
- ConnectIPPBXTransit
- ConnectTransitToVMSvr
- AddCountryTransits
- AddCustomer

- AddVMService
- AddVMServicePilot
- AddVMServicePilotIPPBX
- AddConferenceSvc
- AddConfSvcPilot
- AddAAServicePilot
- AddAAServicePilotIPPBX
- AddLocation
- ConnectLocation
- AddLocationVM
- AssociateFNN
- AddPSTNPubNum
- AddInternalPubNum
- AddEmergNum
- AssocPortLocation
- AddTransitLocalArea
- AddInternationalGWUsage
- ConTransPBXGwPriTransit
- ConnectIPPBXLocation

Activating the PGW Export Functionality

Procedure

A system level preference *AllowPGWexport* enables or disables the export tool. To enable or disable the *PGW Export* tool:

- Step 1** While logged in as a System level user, browse to *Setup Tools > Global Settings*.
- Step 2** Select the *AllowPGWexport* preference.
- Step 3** **Enable** the preference. The PGW Export functionality will now be active within the system.
-

Exporting MML and Times Ten data

Procedure

Use the tool as follows:

- Step 1** Browse to *Network > Transit Switches* and select the required Provider.
- Step 2** Select the required *PGW* then click the **Export** button.

Note

The export button is located at the bottom of the screen, if it is not visible, you may be required to scroll down to the bottom of the page.

Step 3 Select all of the required fields then click the **Export** button.

Two key files will be generated, namely *pgw.txt* and *pgwtimes10.txt*. The files will be written to the */data/nfs/share/usm/export* directory within the system's platform. The directory name and export file names cannot be changed. An Apache alias has been setup and these files can be accessed from the system GUI via the hyperlinks supplied on the *Export PGW Data* screen.

Certain transactions will write to the PGW Times Ten file. In this case, the file will be split into smaller files and a command file after all the transactions have run successfully. The command file (*import_times10_data*) can be used to import the Times Ten files once transferred to the new PGW server. The size of the split files can be changed using the *DriverMaxBulkEntries* model entry in the PGW Times Ten model. The directory for the split files is (*/data/nfs/share/usm/export/split*) and the naming convention used for the split data files is *export00000 - export99999* and *import_times10_data* for the command file. The split data files and command file are also compressed into a ZIP file (*PGW_Times_Ten.zip*) which can be transferred and unzipped in the */opt/CiscoMGC/etc/cust_specific/* directory on the PGW.

AssociateFNN

Note

For more in depth information regarding AssociateFNN, please see the standalone *Associate FNN Guide*.

The *associateFNN* transaction handles the mapping of external numbers (Also known as FNNs) to internal numbers (Also known as FINTs). The functionality allows for a single FNN to be mapped to a FINT or multiple FNNs to be mapped to the same FINT. The mapping of a single FNN to multiple FINTs is not supported. This feature has a number of related settings and is supported in several areas in the product such as *Location Administration* as well as *Voicemail* and *Conference* services.

Voicemail and Conference Services

Once numbers are moved to these services, they can be associated with pilot numbers configured for the service. They cannot be associated with numbers that have not been configured as pilots for the service.

Note

- The system allows for the ability to associate FNNs from any available country to a Voicemail Service.
- PGW MML driver has not been tested and should not be considered to support FNN transaction.

General Rules

The following general rules apply:

- AssociateFNN called for all FNNs and should configure inbound call routing number mapping.

- Primary models called only for the primary FNN and configure outbound call routing CLI selection.
- Redirect models called for Primary FNNs only.
- Emergency models called for Primary FNNs only.

Cloned Line (Multiline) Functionality

The *cloned lines* feature provides the ability to clone one or more lines, multiple times for a phone or an extension mobility profile. A clone is an exact copy of the original line being cloned. Cloned lines and their clones have a Busy Trigger of 1 and the Call Forward Busy of each clone is set to the next clone. The purpose of this feature is to compensate for the lack of a Call Waiting feature. Call Waiting will be simulated by the *cloned line* feature with every clone holding one call. If an extra call comes in on a line, it will be delegated to the next available clone. One of the key purposes of the cloned lines feature is so that phones with no call waiting feature can simulate it. Common phones that do not support call waiting include the Cisco 6921, 6941 and 6961 phones.

To activate the cloned line functionality, please ensure the following:

Cloned Line Prerequisites

- The selected Feature Group includes the Cloned line feature.
- The feature group supports more than 1 line.
- The phone button template supports more than 1 line.

Procedure

Registering a Phone

The user has the option of cloning a line as part of the process of selecting lines when registering a phone.

Note

- Each clone will be assigned its own line button on the phone.
- The amount of clones plus the amount of unique and cloned lines will not exceed the amount of line buttons available for the phone being registered.

To register a phone:

Cloning a Line

- Step 1** Browse to *Location Administration > Phone Registration > [Device name]*.
- Step 2** Click the **Next** button to navigate to the second screen of phone registration.
- Step 3** Below each Number select box, there is a Cloned Lines selection box (except for the last Number). Select the number of Cloned Lines required to clone the line.
- If a selected number is shared and has been cloned before, the number in the Number select box will be prefixed by 'Cloned (x)' where 'x' represents the amount of clones associated with the line. If you select a shared line like this, you must clone it the same amount of times as before, otherwise registration will fail.
- Step 4** Click the **Next** button to navigate to the third screen of phone registration.

- Step 5** Select the Line Class of Service for the line(s) you have selected for cloning. The Line Class of Service will be automatically replicated for all the clones of the line. All clones will have the word 'Clone' displayed in their Label field.
- Step 6** Click the **Register** button to complete phone registration.

When unregistering a phone, all cloned lines are automatically unregistered along with other lines.

Important notes when managing a phone with cloned lines:

Managing a Phone

- Line settings can only be changed for the original line, not the clones.
- All line settings changed for a line will automatically be applied to the clones of that line.
- Line details will be suffixed with '(Clone)' if the line in question is a clone.

Procedure

Adding a Line to a Registered Phone

When adding a new line to an already registered phone, the user has the option of cloning the new line.

- Step 1** Browse to *Location Administration > Phone Management > [select Device Name]*.
- Step 2** Click the **Add Line(s)** button.
- Step 3** Click the **Next** button.
- Step 4** Below each Number select box, there is a Cloned Lines selection box (except for the last Number). Select the number of Cloned Lines required to clone the line.
- If a selected number is shared and has been cloned before, the number in the Number select box will be prefixed by 'Cloned (x)' where 'x' represents the amount of clones associated with the line.
- If you select a shared line like this, you must clone it the same amount of times as before, otherwise registration will fail.
- Step 5** Click the **Next** button.
- Step 6** Select the Line Class of Service for the line(s) you have selected for cloning. The Line Class Of Service will be automatically replicated for all the clones of the line. All clones will have the word 'Clone' displayed in their Label field.
- Step 7** Click the **Add** button to complete line registration.

Important notes when deleting lines from a registered phone:

Deleting Lines from a Registered Phone

- Individual clones cannot be deleted from a registered phone.
- When a line is deleted from a registered phone, all clones of that line will be deleted as well.
- Lines listed for deletion that have clones will be suffixed with 'Cloned(x)' where 'x' represents the number of clones.

Procedure

Adding an Extension Mobility Profile

The user has the option of cloning a line as part of the process of selecting lines when creating an extension mobility profile.

Note

The number of clone lines plus the amount of unique and cloned lines will not exceed the amount of line buttons available for the phone type the extension mobility profile is being based on.

To add a Cloned line with an Extension Mobility profile:

- Step 1** Navigate to *Location Administration > End Users > [select Add under Extension Mobility]*.
- Step 2** Click the **Next** button.
- Step 3** Below each Number select box, there is a Cloned Lines selection box (except for the last Number). Select the number of Cloned Lines required to clone the line.
- If a selected number is shared and has been cloned before, the number in the Number select box will be prefixed by 'Cloned (x)' where 'x' represents the amount of clones associated with the line. If you select a shared line like this, you must clone it the same amount of times as before, otherwise registration will fail.
- Step 4** Click the **Next** button.
- Step 5** Select the Line Class of Service for the line(s) you have selected for cloning. The Line Class of Service will be automatically replicated for all the clones of the line. All clones will have the word 'Clone' displayed in their Label field.
- Step 6** Click the **Add** button to complete the process.

When deleting an Extension Mobility Profile, all clones are automatically deleted along with other lines from the extension mobility profile.

Important notes for managing an extension mobility profile:

Managing an Extension Mobility Profile

- Line settings can only be changed for the original line, not the clones.
- All line settings changed for a line, will automatically apply for the clones of that line, if any.
- Line details will be suffixed with '(Clone)' if the line in question is a clone.

Procedure

Adding Lines to an existing Extension Mobility Profile

When adding a new line to an existing extension mobility profile, the user has the option of cloning the new line.

Adding Lines to an existing Extension Mobility Profile:

- Step 1** Navigate to *Location Administration > End Users > [select User Name] -> Extension Mobility Profile*.
- Step 2** Click the **Add Line(s)** button below *Line Details*.

-
- Step 3** Click the **Next** button.
- Step 4** Below each *Number* select box, there is a Cloned Lines selection box (except for the last *Number*). Select the number of *Cloned Lines* required to clone the line.
- If a selected number is shared and has been cloned before, the number in the *Number* select box will be prefixed by 'Cloned (x)' where 'x' represents the amount of clones associated with the line. If you select a shared line like this, you must clone it the same amount of times as before, otherwise registration will fail.
- Step 5** Click the **Next** button.
- Step 6** Select the *Line Class of Service* for the line(s) you have selected for cloning. The *Line Class of Service* will be automatically replicated for all the clones of the line. All clones will have the word 'Clone' displayed in their *Label* field.
- Step 7** Click the **Add** button to complete the process.
-

Important notes when deleting an existing Extension Mobility Profile:

Deleting Line from an existing Extension Mobility Profile

- Individual clones cannot be deleted from an extension mobility profile.
- When a line is deleted from a mobility profile, any and all clones of that line will be deleted as well.
- Lines listed for deletion that have clones will be suffixed with 'Cloned(x)' where 'x' represents the amount of clones.

When a line is added to a pickup group, all clones associated with that line are automatically added as well.

When a line is deleted from a pickup group, all clones associated with that line are automatically deleted from the group as well.

Notes regarding cloned lines and bulk loaders:

Bulk Loaders

- The bulk loaders for Register Phone and Add User Extension Mobility include columns for the cloned line functionality
- Next to each **Line** column, there is also a **Number of Clones** column used to specify how many clones of the line should be made.

Notes regarding cloned lines and web services:

Web Services

- Register Phone and User Mobility both have support for cloned lines.
- The **<numberOfClones>** tag is used underneath the **<lines>** tag to indicate the number of clones in question.

Notes regarding cloned lines and Self Care:

Self Care

- Lines that are presented in the Self Care GUI on the Phones and Extension Mobility screens have an indicator to distinguish them as cloned or not.

- In the **Line Details** section of the **Line** tabs the text 'Cloned x' will be visible where 'x' represents the amount of clones associated with the line.

Support for Cisco Analog Telephone Adaptors (ATA)

The system supports the use of ATA devices via both SIP and SCCP gateways.

Support VIA SIP

The Cisco Analog Telephone Adaptor (ATA) range provides voice-over-IP (VoIP) termination functionality for businesses and home users. What makes this range of products unique is that it is designed to interface analog equipment, such as analog phones and FAX machines, to a next generation VoIP network. Hence, users are able to connect analog equipment to their Ethernet LAN. The system supports the use of the ATA range via a SIP gateway.

Note

The system only supports the ATA 186 device

Procedure

To add an ATA device to your network:

- Step 1** Create the required phone type in the system, for example, *ATA 186 SIP* . This step only needs to be completed once and can be completed when initially loading the platform. For more information, please see the Adding Phone Types section in the Deployment Guide.

Note

When adding a new phone type, please remember to disconnect and then reconnect the dial plan.

For information on the available fields when adding an ATA phone type, see [ATA Device Parameters on page 926](#).

- Step 2** Create a feature group for the ATA devices, for example, *ATA* . See [Feature Group Management on page 500](#) for more details if required.

Due to the nature of ATA devices, the above feature group should not support the following features:

- Operator console
- User mobility
- Label
- SRST
- Auto answer
- Hot line
- Cache username on phone
- Forwarding delay disabled
- Enable PC support
- Enable phone speaker

- Enable phone speaker and headset
- Enable video
- Allow user login to phone
- Logout from hunt groups
- Speed dials
- Busy lamp fields
- No answer ring duration
- Hold reversion ring duration
- Hold reversion notification interval
- Display name (Caller Line ID)
- Line mask
- Ring setting - Phone idle
- Ring setting - Phone active
- Call forward on CTI failure
- Contact Center Agent Line
- Alerting Name

- Step 3** Add the required number of ATA devices to the Provider Inventory using the ATA phone type created in Step 1 above. See [Phone Inventory on page 830](#) for more information if required.
- Step 4** Move the phone to the required location. See [???](#) for more information if required.
- Step 5** Register the phone using the feature group created in Step 2 above. See [GUI Phone Registration on page 781](#) for more information if required.
- Step 6** If you do not already have the required user in your system, create the required end user within the system. See [Add an End User on page 842](#) for more information if required.
- Step 7** Associate the user with the ATA. See [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#) for more information if required.
- Step 8** Configure the ATA via the ATA Web interface. Refer to the "Cisco ATA 186 and Cisco 188 Installation and Configuration Guide" that came with the device for more information if required.

Note

- You are not able to configure the actual ATA device via the system; please configure the ATA device using the ATA device's own web interface.
- The username and password for the ATA interface will be the same as that entered when configuring the phone in the system.

The ATA device will now be configured within the system.

Mobility Connect

This functionality has been introduced to system release 7.3 in order to support Mobile Clients such as iPhone, Nokia S60, CUCIMOC, CUCICONNECT, CUPC SIP etc.

Versions

The Mobility Connect feature has the following requirements:

- The system only supports mobility connect with Cisco Unified Communications Manager (Unified CM) version 8 and above.

Required Plug-ins

For the Nokia clients, the following file needs to be installed on the Unified CM:

- cmterm-nokia_s60_8.0v1-sccp.cop.sgn

For the iPhone, the Unified CM needs the following file:

- cmterm-iphone-install-100222.cop.sgn

These files must be installed on every Unified CM server in the cluster and then they need to be restarted. Without these, users cannot add these phones as Device Types.

Configuring Mobility Phone Type Integration

To enable Mobility Phone type integration, configuration only needs to occur within the system.

Note

- This section assumes that the Mobility Phone Types have already been loaded using the bulk loaders as specified in the Bulk Loader section above:
 - The following steps can also be performed using the Bulk Loaders: 7-Divisions.xml and 9-LocAdmin.xml
-

Procedure

To configure Mobility Phone Type Integration:

- | | |
|---------------|--|
| Step 1 | Browse to <i>Location Administration > Phone Inventory</i> . |
| Step 2 | Click the Add Phone button to navigate to the <i>Add Phone</i> screen. |
| Step 3 | Depending on the phone type selected from the drop down list, the MAC address, or device name fields is displayed as is applicable to the selected phone type. |
| Step 4 | Once the new phone type has been added, it can be moved to a location by selecting the phone from the Phone Inventory list and selecting the target from the drop down list, or alternatively selecting the phone from the Resources > Phone Inventory page. |
| Step 5 | Register the phone using the <i>Location Administration > Phone Registration</i> menu. The registration process prompts for the necessary extensions to be selected together with other values required to configure this specific line. |
-

Eventing

Eventing is a feature that assists with managing eventing subsystem configuration as well as managing configuration, regeneration and resubmission of notifications. The main purpose of the eventing subsystem is to ensure that a third party database remains in sync with the system. The eventing system has been designed to accommodate various plug-ins from different vendors.

While the core role is for billing purposes related to IP devices and services, the information can be used for other purposes.

The Eventing system consists of two core parts:

- Event handling
- Process notifications from the events

Procedure

View configured eventing subsystems

To view configured eventing subsystems within the system:

- Browse to *Setup Tools > Eventing*.

The *Eventing Subsystems* page lists all of the current event subsystems configured within the system.

Information on this page includes the name of configured subsystems, the trigger levels and the status of the triggers.

Note

The *Trigger on* field will either be *Global* or it will contain a hierarchical identifier, for example, *Provider1*, *Reseller1*.

Procedure

Viewing the details of an Eventing subsystem

To view the details of a single Eventing subsystem:

- Step 1** Browse to *Setup Tools > Eventing* .
- Step 2** Select the relevant **Eventing Subsystem** (active text link). The details of the selected Eventing subsystem will be displayed.

This includes a table containing a list of events and their related actions. This information cannot be edited here and is for information purposes only.

Procedure

Enabling a Trigger Level

To enable a trigger level:

- Step 1** Browse to *Setup Tools > Eventing* .
- Step 2** Click the **Enable Trigger Level** button.
- Step 3** Select the required subsystem, and then click the **Next** button.
- Step 4** Select the relevant entities in the system hierarchy, and then click the **Add** button. The Eventing sub-level will be added to the system.

Procedure

Disabling a Trigger Level

To disable a trigger level:

- Step 1** Browse to *Setup Tools > Eventing* .
- Step 2** Click the **Disable** button adjacent to the subsystem that you would like to disable. The subsystem will be removed from the system.

Licensing

Licenses are managed at Customer and Location levels.

The *Customer License Management* page allows administrators to enable particular license types for their locations, and to indicate which license types are billable.

The *Location License Management* page enables administrators to manage the licenses available within a location.

Enabling/Disabling License Types

Procedure

To manage the allowed license types:

- Step 1** Navigate to *General Administration > Customers* .
- Step 2** Select a customer then click the **Advanced Mgt.** button
- Step 3** Click the **License Management** button.
- Step 4** Select the OSS/BSS License Module(s) for the Customer. The following options are available:
- General License Management
 - License Management GUI
- Step 5** Associate License/Service Types to the Customer, by completing the following fields:

Field	Description
Enabled	Checkbox (select to set) to offer service/license type at customer.
Billable	Checkbox (select to set) to indicate whether service/license type will be billable.
Services/License Types	A list of the type of services/licenses available.
Number of Licenses Used	Number of licenses already in use at the customer.
Number of Licenses Reserved	Total number of licenses available to the customer, based on license orders.
Description	A description of when individual licenses will take effect.

Available License/Service Types

Service/License Types	Description
HUCS Seat	This type does not apply to Cisco HCS.

Service/License Types	Description
HUCS Web Conferencing	This type does not apply to Cisco HCS.
HUCS IP Video	This type does not apply to Cisco HCS.
HUCS Attendant Console	This type does not apply to Cisco HCS.
HUCS Auto Attendant	This type does not apply to Cisco HCS.
HUCS Fixed Mobile Convergence	This type does not apply to Cisco HCS.
HUCS IP Fax	This type does not apply to Cisco HCS.

Note

- For a Service/License Type to be Billable, it has to be checked as both Enabled and Billable for the customer.
- When a Service/License Type is enabled but not billable, the customer will still need licenses for the service, but will not need to go through the system's online process of requesting a quote and placing an order for licenses.

Step 6 The *Enable Selfcare Translation* and *Enable Phone Interface Translation* checkboxes are pre-selected and deactivated, which means that both Self Care and Phone interfaces will be translated into the selected languages.

Select the *Enable Admin GUI Translation* checkbox to enable all Admin GUI screens to also be translated into the selected languages.

Step 7 Associate Language Licenses to the Customer by selecting the required languages from the *Available Languages* list. To select a language, click on the relevant language(s) and click the **Assign >>** button.

Step 8 Select the default language for the Customer by clicking on a relevant language in the *Selected Languages* select box and clicking the **Move Up** or **Move Down** button. The first language on the Selected Languages list will be the default language for the customer.

Note

- English (United States) will always appear on the Selected Languages list.
- A customer's default language can be overridden per location, per user and per phone by another licensed language. The language hierarchy starts with the customer at the top, followed by location and end user/ phone. Each level/entity's default language becomes the next level/entity's default language, until it is overridden with another language, which then becomes the language for that level/entity as well as the default language for the next level/entity.
- The location's default language can be overridden by another licensed language selected for or by the end user. When a language has been selected for an end user, this language overrides the location's default language. When no language has been selected for an end user, the location's default language will be used.
- Similarly, customer administrators can override the customer's default language and location administrators can override the default language of the location.
- The language on the phone interface can also be set to override the default languages set at other levels of the hierarchy. If the override language is not set for the phone, then the location's default language will apply to the phone; if the location's language is not set, then the customer's default language will apply to the phone. The language which is set for the

phone on Cisco Unified Communications Manager is synchronized with the language set in the system.

- Step 9** Click the **Modify** button. The Customer's licensing details, including the list of available languages, will be modified.

For more information on multi-language support in the system, please see the "Multi-Language Support Guide".

Viewing Available Licenses

Procedure

To view licenses available in the location:

- Step 1** Navigate to *Location Administration > Licenses* .
- Step 2** If required, browse through the relevant hierarchies to the required Location. The page will display all available licenses for the location:

Field	Description
Services/License Types	The name of the service/license.
Used	The number of service/licenses currently in use.
Remaining	The number of service/licenses remaining to be used.
Reserved	The number of service/licenses reserved for this location.
Description	A description of the service/license.

Refreshing the *Location License Management* page

Procedure

To refresh the list of available licenses on the *Location License Management* page:

- Step 1** Navigate to *Location Administration > Licenses* .
- Step 2** If required, browse through the relevant hierarchies to the required Location.
- Step 3** Click the **Refresh** button. The list of available licenses will be refreshed.

Requesting a Quote For License Updates

Procedure

To request a quote for license updates:

- Step 1** Navigate to *Location Administration > Licenses* .
- Step 2** Click the **Update** button. The following fields are available:

Field	Description
Services/License Types	The name of license.

Field	Description
Used	The number of licenses currently in use.
Remaining	The number of licenses remaining to be used.
Reserved	The number of licenses reserved for this location.
Update Quantity	A number by which to modify the number of reserved licenses.
Action	The action that will be taken when the licenses are updated: <ul style="list-style-type: none"> • Install • Modify • Disconnect
New Amount Reserved	The number of licenses that will be reserved after the update.

Step 3 Modify the relevant fields then request the quote by clicking the **Request Quote** button.

Step 4 After a quote has been requested, the following details are displayed:

Services/License Types	The name of license.
Number of licenses Currently Reserved	The number of licenses currently reserved.
Number of licenses Updates Requested	The number of license updates requested.
Number of licenses Reserved after updates	The number of licenses that will be reserved after the update.
Per unit cost of updates Non Recurring	The per unit non-recurring cost of the updates.
Per unit cost of updates Monthly Recurring	The per unit monthly-recurring cost of the updates.
Total cost of updates Non Recurring	The total non-recurring cost of the updates.
Total cost of updates Monthly Recurring	The total unit monthly-recurring cost of the updates.
Total monthly recurring costs Current	The current total monthly-recurring costs.
Total monthly recurring costs After updates	The total monthly-recurring costs after the updates.

Step 5 Click the **Cancel Order** button to cancel the order (optional).

Note

A request for a quote cannot be done when there is any order still pending.

Submitting an Order

Procedure

To place an order after receiving a quote:

Step 1 Navigate to *Location Administration > Licenses* .

- Step 2** Select the required *quote* (active text link).
- Step 3** Click the **Submit Order** button on the requested quote page. You will be asked to confirm the order before submitting the order .

After the order has been processed, a **status message** is displayed.

Meet-Me

The Meet-Me implementation is a feature used to reserve internal numbers for Cisco Meet-Me conference numbers.

The Cisco Meet-Me number facility is used as an "always on" conferencing facility, where unlike ad hoc conferencing, no initiator needs to start the conference and participants join by simply dialing the Meet-Me extension from the Meet-Me menu option on their phone.

Meet-Me Numbers cannot be shared by Phones, Extension Mobility Profiles, Line/Number Groups, Pickup Groups and the like and are therefore unavailable to any other system entity. Therefore, when an extension is used for Meet-Me in the system, it is marked as reserved for Meet-Me and configured on the Cisco Unified Communications Manager as such and is prevented from being assigned to other system entities within the system.

Procedure

Viewing Configured Meet-Me Numbers

The *Meet-Me Number Management* page enables users to view and manage existing Meet-Me numbers as well as configure new Meet-Me numbers within the system.

To view configured Meet-Me numbers within the system:

- Step 1** Browse to *Location Administration > Meet-Me* configuration OR browse to *Location Administration > Telephony > Meet-Me*. This page lists all configured Meet-Me numbers.
- Step 2** Select the *Internal Number* (active text link) of the Meet-Me number that you would like to view the details for. The resulting page displays the Extension, Location and Description of the selected Meet-me number. From here, users are able to view, edit and delete the selected Meet-Me number. If you would like to modify the Meet-Me number, make the required changes then click the **Modify** button.
-

Adding a Meet-Me Number

Procedure

Meet-Me numbers are added via the *Meet-Me Number Management* page in the system.

To add Meet-Me numbers to the system:

- Step 1** Browse to *Location Administration > Meet-Me* Configuration OR browse to *Location Administration > Telephony > Meet-Me*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields, and then click the **Next** button.
- Step 4** Complete all of the required fields. The following fields are available when adding a Meet-Me number:

Field	Description	Remarks
Start Extension	The initial extension for the range.	Select from the drop-down list.
Range	The size of the range. Available range sizes are between 1 and 10.	Select from the drop-down list (between 1 and 10).
Description	An optional description for each Meet-Me number	Enter description as required.

Step 5 Click the **Submit** button. The Meet-Me number is added to the system.

Managing a Meet-Me Number

Procedure

Modifying Meet-Me Numbers

To modify Meet-Me numbers:

- Step 1** Browse to *Location Administration > Meet-Me Configuration* OR browse to *Location Administration > Telephony > Meet-Me*.
- Step 2** Select the *Internal Number* (active text link) of the Meet-Me number that you would like to modify.
- Step 3** Make the required changes to the fields as described in [Adding a Meet-Me Number on page 376](#)
- Step 4** Click the **Modify** button. The Meet-Me number is modified in the system.

Procedure

Deleting Meet-Me Numbers

Meet-Me numbers are deleted via the *Meet-Me Number Management* page in the system.

To delete Meet-Me numbers from the system:

- Step 1** Browse to *Location Administration > Meet-Me Configuration* OR browse to *Location Administration > Telephony > Meet-Me*.
- Step 2** Select the *Internal Number* (active text link) of the Meet-Me number that you would like to delete.
- Step 3** Click the **Delete** button. The Meet-Me number is deleted from the system.

Bulk Loading Meet-Me Numbers

Meet-Me numbers can also be managed via the bulk-loaders. This is done using the *Add Meet-Me Numbers* sheet located in the *09-LocAdmins* workbook.

Available columns include:

- Provider Name: The Provider where the fint range is located
- Reseller Name: The Reseller where the fint range is located
- Customer Name: The Customer where the fint range is located

- Division Name: The Division where the fint range is located
 - Location Name: The Location where the fint range is located
 - Extension Ranges: The extension or extension range in one of the following formats:
 - Single Extension, DDI or internal number EXT:12345, DDI:12345, INT:12345
- Extension ranges Contained in comma separated list e.g. 0013-0014, 0015-0016
- Description: The Meet-Me number description. When bulk loading ranges, all Meet-Me Numbers receive the same description.

Managing Phone Services

The system provides functionality to configure and manage IP Phone Services and to subscribe end user devices and mobility profiles to these services.

This includes the ability to import existing configured IP Phone Services from a Cisco Unified Communications Manager (Unified CM) into the system. In addition to the service configuration (Add/Modify/Delete) on a specific Unified CM, admin users can also apply ('push') existing configuration(s) onto multiple Unified CM clusters from a configured 'parent' Unified CM.

Procedure

The workflow summary is as follows:

- Step 1** Import existing IP Phone services from a Unified CM.
 - Step 2** Manage existing or configure new IP Phone service for a Unified CM.
 - Step 3** Push/apply configurations onto other Unified CM clusters.
 - Step 4** Subscribe devices or mobility profiles to the IP Phone Services.
-

Procedure

Importing IP Phone Services from a Cisco Unified Communications Manager (Unified CM)

To import IP Phone Services from a Unified CM:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Select the relevant server *name* (active text link).
 - Step 3** Click the **IP Phone Services** button.
 - Step 4** Click the **Import from CUCM** button.
-

This imports the IP Phone Services from the parent Unified CM and updates the settings and parameters for each Phone Service.

Phone and extension mobility profile subscriptions to the imported services are also updated in the system.

Certain services, namely Voicemail, Login/Logout, Roaming Login/Logout, and Phone Services are restricted from being deleted from the system, since devices and extension mobility profiles are automatically subscribed to them based on established workflows.

Phone Services which were previously associated with the parent Unified CM which are not present upon import are removed from the system (together with any profile subscriptions to them). The import button therefore performs a sync function.

Failure Conditions

- The import fails if one of the services on the parent Unified CM is set to a Service Category or Service Type that does not exist in the system.
- Although the Unified CM has no criteria for uniqueness of a Phone Service, the system determines that no two Phone Services can have the same name and URL. If, on import, two or more of the Phone Services fail this uniqueness rule, that is have the same Name and URL, then none of these potentially duplicate services are imported. The transaction result shows a warning that a service has been duplicated, together with the offending name and URL. Other non-duplicate services and their relevant descriptions are however imported.

Procedure

Adding an IP Phone Service

To add IP Phone Services:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant server *name* (active text link).
- Step 3** Click the **IP Phone Services** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields in the *Service Information* section. Available fields include:

Field	Remarks
Locale	A drop-down list with the locale options imported from Unified CM. This is a mandatory field. Select the associated checkbox to set the locale as the default for the service (optional).
Parent Container	Services can be added to new containers. This is a mandatory field.
Service Name	The name of the service. This is a mandatory field.
ASCII Service Name	An ASCII value for the name of the service. This is a mandatory field.
Service Description	A description for the service.
Service URL	The URL associated with the service. This is a mandatory field.
Secure-Service URL	An alternative service URL normally starting with https://
Service Category	Select from the drop-down list the category of service. This is a mandatory field.
Service Type	Select from the drop-down list the service type. This is a mandatory field.
Service Vendor	The vendor of the service. This is a mandatory field if service category type <i>Java MIDlet</i> is selected (see above field).
Service Version	The version of the service. Allowed characters: 0-9 and '.'
Enable	Select the checkbox to enable the service.
Enterprise Subscription	Select the checkbox to set the service as an enterprise subscription. Only available when adding a service (cannot be modified).

- Step 6** Complete the required fields in the *Attributes Info* section of the screen.

Multiple parameters can be added to a service. Each parameter is added individually. After the details of a parameter are entered, click the **Add** button in the *Attributes Info* section. The parameter is now displayed in the *Attributes List* section, from where it can be deleted or modified.

To delete a parameter: In the *Attributes List* section, select the radio button next to the required parameter and then click the **Delete Parameter** button adjacent to the required parameter in the *Attributes List* section.

To modify a parameter: Select the required parameter *name* (active text link) in the *Attributes List* section; the parameter's details are now displayed in the *Attributes Info* section. Modify the relevant field values and then click the **Modify** button in the *Attributes Info* section. After the **Modify** button is clicked, the fields are empty again and the **Modify** button is replaced by an **Add** button, to enable the admin user to add a new parameter.

Available fields include:

Field	Remarks
Parameter Name	The name of the parameter. This is a mandatory field.
Parameter Display Name	The name of the parameter which should be displayed to the user. This is a mandatory field.
Default Value	A default value for the parameter.
Parameter Description	A description for the parameter. This is a mandatory field.
Parameter is required	Select the checkbox to indicate that the parameter is required.
Parameter is a Password (mask contents)	Select the checkbox to indicate that the parameter is a password.

Step 7

To save new parameters or updates to parameters, click the **Add** or **Modify** button at the bottom of the *Attributes Info* section of the screen.

Procedure

Modifying an IP Phone Service

To modify an IP Phone Service:

Note

- All services are available to be viewed and modified from within Cisco Unified Communications Domain Manager (CUCDM).
- Changes to parameters are only implemented when the entire form is saved, and not as each individual change is made.
- The Enterprise Subscription setting cannot be modified and parameters are not allowed on Enterprise Subscription services.
- Phone and extension mobility profile subscriptions on the Cisco Unified Communications Manager (Unified CM) are updated with the changes by pushing an "Update Subscriptions" command to the Unified CM.
- If the name of a restricted service is changed to one that is not in the list of restricted service names, then the phone service becomes an unrestricted service that can be managed by the administrator in CUCDM, although there will not be any record of the current subscriptions to this service. Only subscriptions that have been explicitly set in CUCDM by the administrator can be managed. A service is restricted when the name of the service matches any of the

following model-driven global settings as per Leaf Cluster Model workbook (see *Call Manager Model Guide*): USM Services, Roaming Login/Logout Name, Login/Logout, or Visual Voicemail

When customizing restricted service names, the recommended procedure is to update and bulk load the global settings in the models first, then modify the IP phone service name via CUCDM.

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant server *name* (active text link).
- Step 3** Click the **IP Phone Services** button.
- Step 4** Select the relevant service *name* (active text link).
- Step 5** Modify the settings for the service.
- Step 6** Click the **Modify Service** button.

Procedure

Translating / Cloning an IP Phone Service

Since locale specific services are merely instances of another phone service within the same container, the CUCDM provides a quick means to clone a service to the host Unified CM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant server *name* (active text link).
- Step 3** Click the **IP Phone Services** button.
- Step 4** Click the required *Translate/Clone* (active text link) in the *Enterprise Service* column.
- Step 5** A pre-populated form, similar to the add page, is displayed. Enter the locale specific settings (Service Name, ASCII Service Name and Description.)
 - The details are pulled from the container's default service. The locale drop-down list options are restricted to those not currently in use by the parent container.
 - The container can't be changed on translation/cloning.

Procedure

Deleting an IP Phone Service

Note

Restricted services cannot be deleted from within the system.

To delete an IP Phone Services:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant server *name* (active text link).
- Step 3** Click the **IP Phone Services** button.

Step 4 Select the required service *name* (active text link) that you wish to delete.

Step 5 Click the **Delete** button.

Procedure

Pushing/Applying IP Phones Services to a different Cisco Unified Communications Manager (Unified CM)

Note

It is preferable to do an import first on each of the cluster's services, prior to performing the push/apply to another Unified CM. This ensures that the system and Unified CM remain in sync, minimizing potential transaction failures.

To push IP Phone Services to a different Unified CM(s):

Step 1 Browse to *Network > PBX Devices*.

Step 2 Select the relevant server *name* (active text link).

Step 3 Click the **IP Phone Services** button.

Step 4 Select the checkboxes associated with the services to push across to the different Unified CM(s).

Step 5 Select the *Apply Phone Services to other CUCM clusters?* checkbox.

Step 6 In the *Managed Remote PBX* section of the screen, select the checkbox(es) associated with the Unified CM clusters to push the services to.

Step 7 Click the **Apply** button.

Note

- Services new to the cluster are added, services already existing on the cluster are modified. Uniqueness of a service on a cluster is determined by name and URL. URLs are re-written where appropriate to match the details of the new cluster
 - New services with locales that don't exist on the destination cluster are sent through with locale set to 'None'. Locales of existing services are not changed.
 - New containers are created when new services are added. Containers are not changed when services are modified.
 - The push/apply process schedules '*child*' transactions to add or modify each service being pushed across onto each of the new clusters. This is to ensure that correct rollbacks occur should failures occur.
-

URL Rewriting. When pushing a service or services from one Cisco Unified Communications Manager (Unified CM) to another, the URL and secure URL fields are inspected before the final push is made. If either URL contains the system's hostname or service IP address, the service is pushed as is. If either URL contains the IP address of the Unified CM being pushed from, the URL is rewritten to replace the home Unified CM with the remote Unified CMs IP address. This is done to ensure that service URL's remain consistent and are based destination Unified CM.

Enabling IP Phone Services in a Feature Group

Procedure

To enable IP Phone Services in a Feature Group:

- Step 1** Browse to *General Administration > Feature Groups*.
 - Step 2** Select the Feature Group *Name* (active text link) to be enabled for IP Phone Services.
 - Step 3** Select the *IP Phone Services Management* checkbox in the *Value Add* section to enable the feature.
 - Step 4** Click the **Modify** button.
-

IP Phone Service subscription management

There are two ways of adding and resubscribing phones and extension mobility profiles to IP Phone Services, namely by way of the **Add and Resubscribe** button (for translated/cloned phone services) and by way of the **Resubscribe All** at the network management level. This can also be done for individual phone / extension mobility profiles at the location level.

Procedure

To resubscribe all devices to the IP Phone Services subscription:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Select the required server *name* (active text link).
 - Step 3** Click the **IP Phone Services** button.
 - Step 4** Click the **Add** button to add a new service to the device.
 - Step 5** Enter the required service details.
 - Step 6** Click the **Add** button at the bottom of the screen.
-

See also [???](#).

Modify container details

Services are now grouped into containers for managing translations of a single service. The names and descriptions of the containers can be modified by clicking on the names of the container and making the changes in the following form.

Note

Container name is mandatory and needs to be unique for a specific cluster within a provider.

Container Rules:

- A container may only contain one 'None' Locale unless an import was done and multiple phone services were collated into one container.
- A container must contain at most one default value.
- If a container has a 'None' Locale, then the 'None' Locale must be the default. In the event that a container has more than one 'None' Locale, the first of the two should be set to default.
- A container may only contain one instance of each language or translation including a 'None' Locale.

- When changing the default value of a container (in the absence of a 'None' Locale) the default is moved i.e. unassigned from service A and assigned to service B.
- Moving a phone service into another container is not allowed if the 'None' Locale is set.
- Moving a phone service into another container is allowed only if the language being moved does not exist in the destination container.
- Moving a phone service with the default value set to another container results in the default being dropped. The container being moved from has a new default set by selecting the language which throughout all containers has the most defaults set, otherwise select randomly.
- All new phone services get added into their own new container, unless the name of the service corresponds to an existing container name. In this case, the new service gets added into the existing container if and only if that container does not already contain a 'None' locale of the newly added service.
- When cloning a service, the service can only be put into the container currently being cloned from.

IP Phone Service Subscription Management for Individual Devices

Phones can be subscribed, unsubscribed and re-subscribed to IP Phone Services.

Procedure

Subscribing a Device to an IP Phone Service Subscription

To subscribe a device to an IP Phone Service subscription:

- Step 1** Browse to *Location Administration > Phone Management*.
 - Step 2** Select the *Device Name* (active text link) to be modified.
 - Step 3** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
 - Step 4** Click the **Subscribe** button to add a new service to the device.
 - Step 5** Select the required phone service group from the drop-down list.
 - Step 6** Click **Next** button.
 - Step 7** Select the required phone service from the drop-down list.
 - Step 8** Click the **Submit** button.
-

Procedure

Unsubscribing a Device from an IP Phone Service Subscription

To unsubscribe a device from an IP Phone Service subscription:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the device to be modified.
- Step 3** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
- Step 4** Select the *Unsubscribe* active text link adjacent to the relevant phone service to unsubscribe the device.

Note

Enterprise Subscription services are shown for informational purposes only. Subscription details for these cannot be changed.

Procedure***Resubscribing a Device to an IP Phone Service Subscription***

This feature is used to align the IP Phone service with the correct service based on the device locale. If the phone changed its locale say from English to German, and it is subscribed to a set of IP Services, the resubscribe function unsubscribes the phone from all services and then subscribes it again but to the services in German. This feature can be done from IP Phone Services for all devices of a Unified CM in case a new language services has been added OR from an OPS Tool for all devices in a location. To resubscribe all the IP phone services for a device:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the *Device Name* (active text link) of the device to be modified.
- Step 3** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
- Step 4** Click the **Resubscribe** button.

This transaction subscribes the device to the correct translation of the service and unsubscribes the 'incorrect' services based on the device locale settings.

Manage IP Phone Service Subscriptions

Extension mobility profiles can be subscribed, unsubscribed and re-subscribed to IP Phone Services.

Procedure***Subscribing an Extension Mobility Profile to an IP Phone Service Subscription***

To subscribe an extension mobility profile to an IP Phone Service subscription:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the relevant end *Username* (active text link).
- Step 3** Click the **Extension Mobility Profile** button.
- Step 4** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
- Step 5** Click the **Subscribe** button to add a new service to the device.
- Step 6** Select the required phone service group from the drop-down list.
- Step 7** Click the **Next** button.
- Step 8** Select the required phone service from the drop-down list.
- Step 9** Click the **Submit** button.

Procedure

Unsubscribing an Extension Mobility Profile from an IP Phone Service Subscription

To unsubscribe an extension mobility profile from an IP Phone Service subscription:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the relevant end *Username* (active text link).
- Step 3** Click the **Extension Mobility Profile** button.
- Step 4** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
- Step 5** Select the *Unsubscribe* active text link of the service to unsubscribe the extension mobility profile.

Procedure

Re-subscribing an Extension Mobility Profile to an IP Phone Service Subscription

To re-subscribe all the IP phone services for an extension mobility profile:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the relevant end *Username* (active text link).
- Step 3** Click the **Extension Mobility Profile** button.
- Step 4** Click the **IP Phone Services** button (in the *IP Phone Service Subscriptions* section).
- Step 5** Click the **Resubscribe** button.

This transaction subscribes the extension mobility profile to the correct translation of the service and unsubscribe the 'incorrect' services based on the extension mobility profile's locale settings.

Leaf Cluster Overview

Leaf Clusters was introduced in order to support Customers who might have more than one IPPBX and want to connect them to each other to avoid the need for routing inter-site calls via the aggregation layer. This is achieved by creating Route Patterns, on each connected Leaf Cluster, that point to the Site Codes of all the Locations that are configured on other connected Leaf Clusters. These are created during the *Connect* transaction, as well as when a new site gets created on a Leaf Cluster that is connected.

Note

This feature replaces the previous procedure of having to connect PBX's to each other using the PGW or any 3rd party aggregation layer device.

For this release, the trunks, Route Groups and Route Lists do not get created automatically, and therefore there are a couple of manual steps to complete the connection process.

Since these steps are manual, it is possible to create any trunk/route group/route list combination suitable for the environment. The example below will outline a basic procedure to integrate with SIP trunks. The models provided do however point to a specific Route List, based on certain values in the system.

Procedure

Static (Cisco Unified Communications Manager) Configuration

Basic outline of the procedure to integrate with SIP trunks:

- Step 1** Add a SIP trunk for every cluster you are connecting to (do this on all clusters you are connecting to, and where you want two-way connectivity).
- Trunk Settings:
- Name: SIP-Trunk-To-Cluster2 (any name that is descriptive to you)
 - DevicePool: GL-DP-Trunk (this device pool would have been created by the system and will be selectable)
 - Inbound CSS: InterSiteRoutingCSS (this would have been provisioned via the model and will be available for selection) Note: Unselect All Transformation CSS's
 - Destination Address: IP Address of Remote Cluster you are connecting to
 - SIP Trunk Sec Profile: Non Secure SIP Trunk Profile
 - SIP Profile: Standard SIP Profile
- Step 2** Create a Route Group for every trunk you have created and select this trunk as your Route Group Member.
- Step 3** Create a Route List for every Route Group added and select this Route Group as your Route List Member. The Route List name needs to be in the following format: RL-TO-*RICPID*. Where *RICPID* the CPID value is of the remote cluster you are connecting to. To get this value in the system, go to *Network->PBX Devices* and Select the PBX you want to connect to. You will see a Value called CPID and a number next to it. This is the number you will use instead of *RICPID*.

Example 2. PBX1 (with CPID= 14) wants to connect to PBX2 (with CPID= 15)

On PBX1 create RL-TO-15. On PBX2 create RL-TO-14

PBX to PBX Connection management

This section covers configuration between managed and unmanaged PBX.

A PBX can be connected to another PBX(s).

Note

This connection type is typically required for Unified CM (ConnectIPPBXIPPBX) models; ConnectIPPBXIPPBX-Unmanaged-SIP, ConnectIPPBXIPPBX-Unmanaged-H323 or ConnectIPPBXIPPBX-SIP, and is used for adding trunks, route groups, route lists, or for Unified CM (AddLocationICTSiteCodes) models; AddLocationICTSiteCodes-Unmanaged-SIP, AddLocationICTSiteCodes-Unmanaged-H323, or LocationICTSiteCodes. Note that the normalization script used must pre-exist, and can be imported from Unified CM, or created in CUCDM on the IPPBX (Cluster Management screen).

Note

A managed PBX can be connected to other managed or unmanaged PBXs, but an unmanaged PBX can only be connected to a managed PBX.

Procedure

Viewing associated PBXs for a managed PBX

To view clusters currently associated to the selected managed cluster:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the cluster that you would like to view.
- Step 3** Click the **PBX==>PBX** button.

A screen will be displayed, with sections, *PBX Clusters Not Connected To <PBX Name>* and *PBX Clusters Currently Connected to <PBX Name>*. The *PBX Clusters Not Connected To <PBX Name>* section lists all PBXs available for connection and the *PBX Clusters Currently Connected to <PBX Name>* section displays the PBX(s) that are currently connected to the selected PBX.

Procedure**Connecting a managed PBX to a managed PBX**

To connect the managed PBX to another managed PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** Click the **Connect IPPBX** button adjacent to the PBX that you would like to associate with the cluster.

Note

To connect multiple PBXs at once, select the checkboxes adjacent to the required PBXs then click the **Connect Selected** button. The **Select All** and **Select None** links can be used when managing multiple PBXs.

The *Manage PBX Server* page will open. This page enables administrators to select whether they would like to just connect the PBXs or connect the selected PBXs with each other and to the selected PBX. The following fields are available:

Field	Notes	Remarks
Trunk Protocol	The trunk protocol.	Select from the drop-down list.
Topology Type	-	Select from the drop-down list. The options include "Star" and "Full Mesh". Star option will result in connectivity between the selected source cluster and the rest of the selected clusters. There will be no connection between the secondary / target clusters. Full Mesh option will connect all clusters participating in the selection between each other as well as the originating cluster. Full Mesh is the default option.
Trunk Name	The available trunks which will be used for the connection between the PBX's.	This is a display field only.

Field	Notes	Remarks
Description	A description of the trunks.	-
SIP Profile	The SIP Profile to apply to the connection.	Select from the drop-down list one of the available SIP Profiles to apply to the connection.
Normalization Script	The Normalization Script to apply to the connection.	Select from the drop-down list one of the available. Normalization Scripts to apply to the connection.
Script Parameters	Key-value pairs to be used by the script.	This is supplied in the format of key=value;key2=value2;key3=value3

Step 5 Click the **Confirm** button. The cluster will now be associated with the selected PBX.

Procedure

Modifying the trunk details of a managed to managed connection

To modify the trunk details of a managed-to-managed connection:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the relevant cluster.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** Click the **Trunk Details** button in the *PBX Clusters Currently Connected to <PBX Name>* section.
- Step 5** Provide the details of the SIP Trunk On the next screen. The following fields are displayed:

Field	Description	Remarks
Trunk Name	The trunk name.	This is a display field only.
Cluster Name	The name of the PBX cluster.	This is a display field only.
Description	A description of the trunk.	
SIP Profile	The SIP Profiles applied to the connection.	Select from the drop-down list one of the available SIP Profiles to apply to the connection.
Select SIP Normalization Script	The Normalization Script applied to the connection.	Select from the drop-down list one of the available Normalization Scripts to apply to the connection.
Script Parameters	Key-value pairs to be used by the script.	This is supplied in the format of key=value;key2=value2;key3=value3, e.g. vendor=cisco;pbx;trunk-id=1234
Script Trace Enabled	The script tracing status.	Select the checkbox to enable script tracing.

Step 6 Click the **Modify** button.

Note

Click the **Reset Trunk** button to reset the trunk's settings.

Procedure

Connecting a Managed PBX to an Unmanaged PBX

To connect the managed PBX to an unmanaged PBX:

Note

When connecting a managed PBX to a managed PBX, the system uses information already provisioned on the system via the bulk loaders (see Bulk loader guide: *Add CUCM Groups*). The transaction *ConnectIPPBXIPPBX* calls the *ConnectIPPBXIPPBX-SIP* model which uses the *#CCMGROUP#* and *#RICPID#* variable. The *#CCMGROUP#* variable will be the value as bulk loaded with *Add CUCM Groups*. This value must match the value configured on Unified CM. However, when connecting to an unmanaged PBX, the transaction *ConnectIPPBXIPPBX-Unmanaged* does not use a *#CCMGROUP#* variable in the model, because unmanaged PBXs are not provisioned via bulk loading, but uses the *#RICPID#* variable when connecting to either a SIP trunk or H323 trunk.

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
 - Step 3** Click the **PBX==>PBX** button.
 - Step 4** Select the checkboxes adjacent to the required PBXs you want to connect the unmanaged PBX to.
 - Step 5** Click either the **Connect SIP trunk** button or the **Connect H323 trunk** button, depending on how you want to connect the two PBX's.
-

Procedure

Disconnecting a Managed PBX from a Managed PBX

To disassociate a cluster from a PBX:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Click the **Connectivity** button adjacent to the Cluster that you would like to modify.
 - Step 3** Click the **PBX==>PBX** button.
 - Step 4** Click the **Disconnect** button adjacent to the PBX that you would like to disassociate from the cluster.
 - Step 5** The Manage PBX Server page will open. This page enables administrators to select whether they would like to just disconnect the PBXs or disconnect the selected PBXs from each other and from the selected PBX.
 - Step 6** Click the **Confirm** button. The cluster will now be disassociated from the selected PBX.
-

Alternatively: To disconnect multiple PBXs at once, select the checkboxes adjacent to the required PBXs then click the **Disconnect Selected** button. The **Select All** and **Select None** buttons can be used when managing multiple PBXs.

The cluster will now be disassociated from the selected PBX.

Procedure

Disconnecting an unmanaged PBX from a managed PBX

To disassociate a cluster from a PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the Cluster that you would like to modify.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** Select the checkboxes adjacent to the required PBXs you want to disconnect the unmanaged PBX from.
- Step 5** Click either the **Disconnect SIP trunk** button or the **Disconnect H323 trunk** button.

Procedure***Viewing associated PBXs for an unmanaged PBX***

To view clusters currently associated to the selected cluster:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the cluster that you would like to view.
- Step 3** Click the **PBX==>PBX** button.

A screen will be displayed, with sections, *PBX Clusters Not Connected To <PBX Name>* and *PBX Clusters Currently Connected to <PBX Name>*. The *PBX Clusters Not Connected To <PBX Name>* section lists all PBXs available for connection and the *PBX Clusters Currently Connected to <PBX Name>* section displays the PBX(s) that are currently connected to the selected PBX.

Procedure***Connecting an unmanaged PBX to a managed PBX*****Note**

An unmanaged PBX can only be connected to managed PBXs.

To associate the unmanaged PBX to a managed PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the PBX that you would like to modify.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** Select the checkboxes adjacent to the required PBXs you want to connect the unmanaged PBX to.
- Step 5** Click either the **Connect SIP trunk** button or the **Connect H323 trunk** button, depending on how you want to connect the two PBX's.

Procedure***Disconnecting an unmanaged PBX from a managed PBX***

To disassociate a cluster from a PBX:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Connectivity** button adjacent to the Cluster that you would like to modify.
- Step 3** Click the **PBX==>PBX** button.
- Step 4** Select the checkboxes adjacent to the required PBXs you want to disconnect the unmanaged PBX from.
- Step 5** Click either the **Disconnect SIP trunk** button or the **Disconnect H323 trunk** button.
-

SME Clusters

UC deployments using Unified CM Session Manager Edition are a variation on the Multi-site Distributed Call Processing deployment model and are typically used where large numbers of UC end systems need to be interconnected via a single UC system - i.e. The Unified CM Session Manager.

Cisco Unified CM Session Manager Edition

A deployment using Cisco Unified CM Session Manager Edition is essentially a Unified CM cluster with trunk interfaces only and with no IP endpoints. It allows aggregation of multiple Unified Communications systems, referred to as leaf systems.

Managing SMEs via Bulk Loaders and Models

SMEs can be managed via the system's bulk loaders, this includes addition of clusters and servers, Modification of clusters and servers and the addition of SME items.

The following bulk loader was updated to cater for the SME functionality within the system:

- *03 - Network HCS*

The following model was added to cater for the SME functionality within the system:

- 2-SME-Model-HCS

Managing SMEs via the system GUI

SME Server Configuration

The screen lists all configured locations and their relevant customers, providers, resellers, customers and divisions.

The information provided on this page includes:

Column	Description
Location Name	The name of the location
Provider Name	The name of the provider responsible for the location
Reseller Name	The name of the reseller responsible for the location
Customer Name	The name of a customer at the location. A single location may have multiple customers.
Division Name	The name of a division within the location.
Address	The address of the Division within the location.

To view further information on a specific location, select the Location Name (active text link) of the location.

SME Cluster Management

To add a cluster, see: [Adding an SME Cluster on page 395](#).

To modify a cluster, see: [Modifying an SME cluster on page 396](#).

To add a server to a cluster, see: [Adding an SME Server to a Cluster on page 393](#).

Procedure

Modifying a Server

To modify a Server:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster that you would like to modify.
- Step 3** Click the **Servers** button.
- Step 4** Select the *Name* (active text link) of the server that you would like to modify.
- Step 5** Modify the required fields and click the **Modify** button. The server will be modified within the SME cluster.

Procedure

Deleting a Server

To delete a Server:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster that you would like to modify.
- Step 3** Click the **Servers** button.
- Step 4** Select the *Name* (active text link) of the server that you would like to delete.
- Step 5** Click the **Delete** button. After confirming the deletion operation, the server will be removed from the SME cluster.

The system enables you to organize your SME servers into groups within a SME cluster.

Adding an SME Server to a Cluster

Procedure

Adding a SME Server

To add a Server:

- Step 1** Browse to *Network > Transit Switches*.

- Step 2** Select the *Name* (active text link) of the SME cluster that you would like to add a server to.
- Step 3** Click the **Servers** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required fields. The following fields are available when adding a Server to a SME cluster:

Note

Depending on the configuration of your system, available fields may vary.

Field	Notes	Remarks
Host Name	Hostname for the server where the Unified Communications Manager is installed.	This is a mandatory field.
SME Name	SME name for the server where the SME is installed.	This is a mandatory field.
Description	A short description of the server.	-
IP Address	The IP address of the server.	This is a mandatory field.
TFTP Server	Select if this server is going to be used as a TFTP Server.	If this option is selected, please provide the order for the server.
Music Server	Select if this server is going to be used as a Music Server.	If this option is selected, please provide the order for the server.
Conference Server	Select if this server is going to be used as a Conference Server.	-
Annunciator Server	Select if this server is going to be used as an Annunciator Server.	-
Media Termination Point Server	Select if this server is going to be used as a Media Termination Point Server.	-
Attendant Console Server	Select if this server is going to be used as an Attendant console Server.	-
CTI Manager Server	Select if this server is going to be used as a CTI Manager Server.	-
MGCP Configured	Select this checkbox if MGCP has been configured.	-
H323 Configured	Select this checkbox if H323 has been configured.	-
SCCP Configured	Select this checkbox if SCCP has been configured.	-
SIP Configured	Select this checkbox if SIP has been configured.	-
Network Monitoring active?	Select this checkbox if you would like the server to activate Network Monitoring.	Note Depending on network loads, selecting this option may impact on the performance of the server.

- Step 6** Click the **Add** button. The server will be added to the SME cluster.

Adding an SME Cluster

Procedure

To add an SME cluster:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Add** button.
- Step 3** When asked to specify what type of server you would like to add, click the **Add** button adjacent to the **SME** server type.
- Step 4** Complete all of the required fields. The following fields are available when adding an SME server:

Note

Depending on the configuration of your system, some of these fields may not be available.

Field	Notes	Remarks
Software Version	This defines the software version running on the SME.	This is a mandatory field. Select from the drop-down list, this must be set correctly to ensure correct operation.
Name	This is the name of the SME.	This field is mandatory and the name provided must be unique within the system.
Description	A short description of the SME.	-
Publisher Host Name	Hostname for the server where the Unified Communications Manager is installed.	This is a mandatory field. Note This should be the actual host-name of the server.
Publisher SME Name	Name for the server where the Unified Communications Manager is installed.	This is a mandatory field.
Publisher IP Address	The IP address of the Publisher.	This is a mandatory field.
Config User ID	The SME server login user name required to configure the SME.	-
Config Password	The SME password, required to configure the SME.	-
Country	Defines the country that the SME is located in.	-
Media Termination Point	Determines if the server is going to be used as a Media Termination Point.	Select this checkbox if the server is going to be used as a Media Termination Point.
Transit switch	Use this field to specify if the server is going to be used as a transit server.	Select this checkbox if the server is going to be used as a transit server.
Manual configuration Mode?	Use this field if the system is not going to be used to configure this device.	Select the checkbox if the system is not going to be used to configure this device.

Field	Notes	Remarks
Email address for Manual activation	If the <i>Manual configuration Mode</i> checkbox is selected, an email address must be entered.	This email address must be of the person/group that will perform the manual configuration of the device.
Network Monitoring active	Select this checkbox if you would like the server to activate Network Monitoring.	Note Depending on network loads, selecting this option may impact negatively on the performance of the server.
Detailed trace file of configuration sessions?	Used to enable the server to maintain a detailed log file of all configuration sessions.	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	Used to ensure that all configuration sessions with the server will be encrypted.	Note While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.

Step 5 Click the **Add** button. The SME will be added to the system.

Modifying an SME cluster

Procedure

Modifying an SME cluster

To modify an SME cluster:

- Step 1** Browse to the relevant sub-menu under the *Network* menu
- Step 2** Select the relevant *SME Cluster* (active text link).
- Step 3** Modify the required fields. The following fields are available when modifying an SME.

Note

Depending on the configuration of your system, some of these fields may not be available:

This screen lists all of the servers configured within the cluster. Details on this page include:

Field	Notes	Remarks
Name	The name of the server.	-
Publisher	Specifies whether the server acts as a publisher.	Options are Yes(Y) or No(N).
IP Address	The IP address of the server.	This must be unique within the system.
TFTP	Specifies whether the server acts as a TFTP.	Options are Yes(Y) or No(N).
Music	Specifies whether the server acts as a Music Server.	Options are Yes(Y) or No(N).
Console	Specifies whether the server acts as a Console Server.	Options are Yes(Y) or No(N).

Field	Notes	Remarks
CTI	Specifies whether the server acts as a CTI Server.	Options are Yes(Y) or No(N).
Description	A short description of the server.	-

- Step 4** Click the **Modify** button. The SME cluster will be modified within the system.

SME Group Management

To add a SME Group, see: [Adding a SME Group on page 398](#)

Procedure

Modifying a SME Group

To modify a group within a cluster:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster that has the group that you would like to modify.
- Step 3** Click the **Groups** button.
- Step 4** Select the *Name* (active text link) of the Group that you would like to modify.
- Step 5** Modify the required fields and click the **Modify** button. The group will be modified within the system.

Procedure

Deleting a SME group

To delete group within a cluster:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster that has the group that you would like to modify.
- Step 3** Click the **Groups** button.
- Step 4** Select the *Name* (active text link) of the group that you would like to delete.
- Step 5** Click the **Delete** button. After confirming the deletion operation, the group is deleted from the system.

Procedure

Adding and Removing a Server(s) from a Group

To modify the servers within a group:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster that has the group that you would like to modify.

- Step 3** Click the **Groups** button.
- Step 4** Select the *Name* (active text link) of the group that you would like to modify.
- Step 5** **Select/Deselect** the checkboxes adjacent to the server names that you would like to add/remove from the group.
- Step 6** Modify the required fields. The information provided on this page includes:

Column	Description	Remarks
Location Name	The name of the location.	-
Provider Name	The name of the provider responsible for the location.	-
Reseller Name	The name of the reseller responsible for the location.	-
Customer Name	The name of a customer at the location.	Note: A single location may have multiple customers.
Division Name	The name of a division within the location.	-
Address	The address of the Division within the location.	-

- Step 7** Click the **Modify** button. The servers is added/removed from the group.

Note

- This page lists all configured locations and their relevant customers, providers, resellers, customers and divisions.
 - To view further information on a specific location, select the Location Name (active text link) of the location. A Transit Server can be associated with an IPPBX.
-

Adding a SME Group

Procedure

To create a new group within a cluster:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Select the *Name* (active text link) of the SME cluster to which you would like to add a group.
- Step 3** Click the **Groups** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields. The following fields are available when adding a group:

Field	Notes	Remarks
Group Name	The name of the group being added.	This is a mandatory field.
Description	A short description of the group.	-
Maximum Streams supported	Specify the maximum number of streams that will be supported by the group.	This is a mandatory field.

Field	Notes	Remarks
Use for Phones	Select this checkbox if this group is going to be used for phones.	-
Use For Trunks	Select this checkbox if this group is going to be used for Trunks.	-
Use For Voicemail	Select this checkbox if this group is going to be used for voicemail.	-
Select Servers	Select the checkbox(s) adjacent to the servers that you would like to appear in this group.	-
Server Order	Use the drop-down list to specify the hierarchy of the servers.	<p>For example, if you would like Server 1 to be before Server 2, you would select 1 from the drop-down list adjacent to Server 1 and you would select 2 from the drop-down list adjacent to Server 2.</p> <p>Important: The server orders must be unique within the group. For example, two or more servers cannot be on order 0. All servers must have a unique order number assigned to them.</p>

Step 6 Click the **Submit** button. The group will be added to the system.

Viewing Associated IPPBXs

Procedure

To view IPPBXs currently associated to the selected Transit Server:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit ==> IPPBX** button adjacent to the SME that you would like to associate/disassociate from a Transit Server(s).

A screen will be displayed, with two columns, one listing the registered (and available) IPPBXs, and the other column will display the servers current connection status. If the button adjacent to the IPPBX says **Connect**, the IPPBX is available for connection. If the button says **Disconnect**, the IPPBX is already connected.

Associating (connecting) a Transit Server to an IPPBX

Procedure

To associate a Transit Server to an IPPBX:

- Step 1** Browse to *Network > Transit Switches*.
- Step 2** Click the **Transit ==> IPPBX** button adjacent to the Transit Server that you would like to associate to an IPPBX.
- Step 3** Click the **Connect** button adjacent to the IPPBX that you would like to connect. The Transit Server will now be associated with the selected IPPBX.

Disassociating (disconnecting) a Transit Server (SME) from an IPPBX

Procedure

To disassociate a Transit Server from an IPPBX:

- Step 1** Browse to *Network > Transit Switches*.
 - Step 2** Click the **Transit ==> IPPBX** button adjacent to the Transit Server that you would like to disassociate from an IPPBX.
 - Step 3** Click the **Disconnect** button Adjacent to the Transit Server that you would like to disassociate from an IPPBX. The Transit Server will now be disassociated from the selected IPPBX.
-

Idle URL Management

This feature provides the ability to configure an Idle URL setting for a phone. This will allow the phone to surf to the URL after the idle timeout in Cisco Unified Communications Manager expires. The sections below outline the steps required to configure this feature. This setting only applies to phones and there are two ways of configuring this for a phone:

- Via the Feature Group
- Individually on the Phone

Adding a Service Type for an Idle URL

The Idle URL you want to offer phones/users needs to be added to the system as a service type. This allows the system to make the Idle URL available to the processes later for assigning to feature groups and phones/extension mobility profiles.

Adding a Service Type

This can be done via the system GUI or the bulk loaders. The GUI is accessible via *Setup Tools > Service Types > Add*. On the add form use the following settings:

- **Service Name:** This is the name of the service type in the system
- **Description:** This is the description of the service.
Note : This will be the text displayed in the feature group for this service type
- **Tag:** Text to identify the service (usually same as service name)
- **Service Category:** Select idleurl from the drop-down.
- **URL :** This will be the URL required. The system will configure this into the Cisco Unified Communications Manager as the idle URL so it should be reachable from the phone (if NAT is used between the phone and the destination, this should be the NAT address the phone will see).
- **Idle Timeout:** This will be the timeout applied to the phone (in seconds).

Note

The other settings are not required and should be left to defaults.

Repeat for each Idle URL required via the feature groups.

Note

This can also be done via the bulk loaders with the *Add Service Types* worksheet.

Managing the Idle URL Setting via the Feature Group

This is the first method of assigning the Idle URL to a phone/user. This feature group method provides the ability to enable the Idle URL for a wide audience of users. This means that any phone/user that using this feature group will be setup with this idle URL by default.

The service is enabled in the feature group via the *General Administration > Feature Groups > Select the Required Feature Group*. The idle URL setting is presented as a drop-down with a default of none. The drop-down contains any service types of the category idleurl added above. Select the required Idle URL from the drop-down. Any existing feature groups can be modified to have a different idle URL setting as required.

Note

Changing the URL setting in a feature group does not immediately apply that setting to the phones using that feature group. The phones would need to be modified to get the new setting.

The phone management screen provides the ability to override the feature group setting. The feature group setting is only used if the phone setting is set to Auto (default). See the next section for more details.

The feature group can also be loaded via the feature group loader. The Idle URL service type required should be included in one of the columns of the loader.

Managing the Idle URL Individually for the Phone

This functionality provides the flexibility of overriding the feature group idle URL setting as required. The Phone Management page (*Location Administration > Phone Management > Select the Required Phone*) provides the following settings related to Idle URL:

- **Idle URL** : This is a drop-down of the options 'Auto', 'None', and any available Idle URL service types. The default setting is 'auto' which means it uses the setting from the feature group.
- **Idle Timeout** : This is a textbox to enter the seconds required for the timeout. This value cannot be empty. Valid settings here are 'auto' or a numeric value for seconds up to a max of 99999. The 'auto' value means the system will use the timeout setting against the idle URL service type selected as the timeout setting.

These settings can also be applied via the *Register Phone* bulk loader worksheet.

Extension Mobility Cross Cluster (EMCC) Configuration

Extension Mobility Cross Cluster extends the system's current extension mobility functionality to allow the user to log in to a device, from within a connected cluster, anywhere in the world. This enables the user to retain the settings, services and lines he/she is familiar with at their home location.

The system automates most of the EMCC provisioning to enable this feature to work on all dial plans across multiple Cisco Unified Communications Manager (Unified CM) clusters that are managed by the same platform instance. A small number of manual configurations remain, specifically around network security, which is outlined in a separate section. The system only automates provisioning of the home cluster in cases where the Unified CM clusters are managed by separate platforms, that is, cross-cluster configuration across multiple platforms is not

supported. To aid this configuration, the system provides a report of the EMCC configuration on the home cluster and information on what needs to be provisioned in the visiting cluster in order to fully support EMCC.

Note

The EMCC feature is only available when using Unified CM version 8.0 or higher.

The following functionality is available from this screen:

- [Home Cluster Setup on page 403](#)
- [EMCC Group Management on page 413](#)
- [View EMCC Configuration on page 412](#)

EMCC Use Case

HOME Cluster	VISITING Cluster
User Profile	Phone (with Geolocation)
Geolocation Filter	
Roaming Device Pool (with Geolocation)	

- A user from the HOME cluster goes to the VISITING cluster and logs onto a phone. The two clusters can be in different countries/territories.
- The user cannot be authenticated in the VISITING cluster, but since the cluster is EMCC enabled, and the phone is subscribed to the EMCC service, the cluster searches for the user in defined EMCC remote clusters.
- Once the user (also subscribed to the EMCC service) is authenticated, the phone is unregistered from the VISITING cluster, and re-registered to the HOME cluster.
- The geolocation of the phone is sent to the HOME cluster. This enables the HOME cluster to associate the relevant roaming device pool to the user's phone using the geolocation filter.
- The phone behaves and dials exactly the same as if the user was logged in at the HOME cluster, and all his/her settings and preferences are preserved.
- Calls to the HOME cluster emergency numbers as well as the VISITING cluster emergency numbers break out at the VISITING cluster (physical location).
- Various other elements such as trunks, EMCC countries, and so on, must be configured on both the HOME-and VISITING clusters to ensure the feature functions.

EMCC Server Setup

At least one server in a cluster must include the EMCC server role in order for the cluster to participate in the EMCC feature, that is, the *EMCC Server* checkbox must be selected (enabled). Servers with this role coordinate communication between clusters configured for EMCC.

Note

EMCC configuration option(s) for a cluster are not available until at least one server in the cluster is configured for the EMCC role (*EMCC Server* checkbox is selected).

Procedure

To enable the server as an EMCC server:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Select the required CCM server *link* (active text link), or add a new CCM server.
 - Step 3** Click the **Servers** button.
 - Step 4** Select the Unified CM Server *Name* (active text link) to manage.
 - Step 5** Make sure that the *EMCC Server* checkbox is selected.
 - Step 6** Click the **Modify** button to save the changes to the database.
-

Note

You can't remove the EMCC role from a server (by modifying or deleting the server) if the server is the last EMCC-enabled server on the cluster, and EMCC group countries are still assigned to the cluster.

To add a new Unified CM server (if required), refer to [Adding a Server to a Cluster on page 81](#).

Home Cluster Setup

The EMCC Home Cluster Setup screen allows the configuration of the individual elements required for Extension Mobility Cross Cluster (EMCC) to function. It also shows a summary of the current configuration in the Configured column. For example, it shows how many EMCC Countries, Remote Clusters, GeoLocations, and Roaming Device Pools are currently configured for the selected cluster.

Note

To enable roaming for a user, a similar configuration is required on the other clusters to which user wants to roam.

EMCC Countries Management

The EMCC Countries screen lists all countries available for the selected provider. Countries currently subscribed for EMCC for this cluster are pre-selected. Additional countries may be selected, or existing countries may be deselected, provided they are not associated with any existing EMCC groups (see also [EMCC Group Management on page 413](#)). Existing group membership is indicated next to each country's checkbox using the name of the EMCC group with which the country is associated. EMCC Countries are required to enable emergency dialing when roaming between clusters.

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required CCM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.

- Step 5** Click the **EMCC Countries** button. The *EMCC Countries* screen is displayed.
- Step 6** Select or deselect the relevant countries by selecting or deselecting the appropriate checkbox adjacent to the required country/countries.
- Step 7** Click the **Apply Subscriptions** button when complete.
-

Remote Cluster Management

If login fails, the system attempt to authenticate the roaming user against the remote clusters specified. This is the first step of the EMCC process, and identifies the roaming user's home cluster.

The *Remote Cluster Management* screen allows the addition of a new remote cluster used for EMCC (Extension Mobility Cross Cluster), or the modification of an existing remote cluster used for EMCC. An existing remote cluster can also be deleted if required.

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required CCM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.
- Step 5** Click the **Remote Clusters** button. The *Remote Cluster Management* screen is displayed.
-

To add new or modify existing remote clusters

Procedure

To add a new remote cluster

- Step 1** Click the **Add** button on the *Remote Cluster Management* screen.
- Step 2** Enter the required parameters in the fields provided (see table below).

Field	Description	Remarks
Cluster ID	The name of the remote cluster.	This is a mandatory field, and can only be modified during the <i>Add</i> process.
Description	Enter a short description of the remote cluster.	This is an optional field, and can only be modified during the <i>Add</i> process.
Fully Qualified Name	Enter the full name to identify the remote cluster.	This is a mandatory field, and can only be modified during the <i>Add</i> process.
EMCC Enabled	Select the checkbox if you want EMCC functionality enabled for the selected remote cluster.	-
PSTN Access Enabled	Select the checkbox if you want PSTN access enabled for the selected remote cluster.	-

Field	Description	Remarks
RSVP Agent Enabled	Select the checkbox if you want RSVP Agent functionality enabled for the selected remote cluster.	RSVP Agent uses Resource Reservation Protocol (RSVP), an IETF standards-based signaling protocol for reserving bandwidth in an IP network.

Step 3 Click the **Add** button when complete. The remote cluster is added to the database.

Procedure

To modify an existing remote cluster

Step 1 Select the relevant remote cluster name *link* (active text link) on the *Remote Cluster Management* screen.

Step 2 Modify the required parameters in the fields provided (see table above).

Step 3 Click the **Modify** button when complete. The remote cluster is modified in the database.

Step 4 Click the **Delete** button **only** to delete the selected remote cluster.

To delete multiple remote clusters, select the checkboxes adjacent to the remote cluster/s to delete on the *Remote Cluster Management* screen, and then click the **Delete** button to delete the selected remote cluster/s. Delete an individual remote cluster (if required) as described in the last step of the previous section.

Geolocation Management

Geolocation is the identification of the real-world geographic location of an object such as a telephone. This can be as general as the continent the device/object is in, or as specific as a particular street address.

To allow the device where a roaming user logs in, to be registered to the correct roaming device pool in the home cluster, both the device and the roaming device pool need must have a Geolocation specified. The Geolocation of the device is determined by the location and/or cluster the device is registered to at the time the roaming user logs in.

The *Geolocation Management* screen allows administrators to add, modify, delete or import geolocations to the cluster, or to 'push' (copy) them to other clusters.

Procedure

Step 1 Browse to *Network > PBX Devices* .

Step 2 Select the required CCM server *link* (active text link).

Step 3 Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).

Step 4 Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.

Step 5 Click the **GeoLocations** button. The *Geolocation Management* screen is displayed.

Procedure

To import geolocations

- The import function copies the geolocations from the Unified CM to the system. If the Geolocation already exists it is overwritten with the information from the Unified CM. Import all geolocations from a specific cluster by clicking the **Import** button on the *Geolocation Management* screen.

Procedure

Push config (geolocations)

Note: The **Push Config** button is inactive until both the geolocations and clusters involved in the 'push' have been selected.

- Click the **Push Config** button to 'push' (copy) a selected list of geolocations to a selected list of clusters. This allows the provider administrator to create the same geolocations on multiple clusters in a single step.

To add or modify a geolocation, see: [GeoLocation Management on page 778](#).

Geolocation Filter Management

The Geolocation filter on a cluster is used to determine which roaming device pool is used to register the device to when a roaming user logs in to the device. Geolocation filters include filters such as *Use Country Code*, *Use State, Region, or Province*, *Use Country or Parish*, *Use City or Township*, etc. Note that only one geolocation filter can be in use at any given time. See also [EMCC Parameters and Profile on page 407](#).

The *Geolocation Filter Management* screen allows administrators to add, modify, delete or import geolocation filters to the cluster, or to 'push' (copy) them to other clusters.

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required Unified CM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.
- Step 5** Click the **GeoLocation Filters** button. The *Geolocation Filter Management* screen is displayed.
-

To add or modify geolocation filters

Procedure

To add geolocation filters

- Step 1** Click the **Add** button on the *Geolocation Filter Management* screen. The *Add GeoLocation Filter* screen is displayed.
- Step 2** Enter the required parameters in the fields provided. Typical fields include: *Name* (mandatory for the Add task), *Use Country Code*, *Use State, Region, or Province (A1)*, *Use County or Parish (A2)*, *Street (A6)*, *Use Name of Business or Resident (NAM)*, and *Use Zip or Postal Code (PC)*.

-
- Step 3** Click the **Add** button when complete. The geolocation filter is added to the database.
-

Procedure

To modify geolocation filters

- Step 1** Select the relevant geolocation filter name *link* (active text link) on the *Geolocation Filter Management* screen.
- Step 2** Modify the required parameters in the fields provided.
- Step 3** Click the **Modify** button when complete. The geolocation filter is modified in the database.
- Step 4** Click the **Delete** button **only** to delete the selected geolocation filter.
-

To delete geolocation filters

Select the checkbox adjacent to the geolocation filter/s to delete on the *Geolocation Filter Management* screen, and then click the **Delete** button to delete the selected geolocation filter/s. Delete an individual geolocation filter (if required) as described in the last step of the previous section.

To import geolocation filters

The import function copies the geolocation filters from the Unified CM to the system. If the geolocation filter already exists it is overwritten with the information from the Unified CM. Import all geolocation filters from a specific cluster by clicking the **Import** button on the *Geolocation Filter Management* screen.

Push config (geolocation filters)

Note: The **Push Config** button is inactive until both the geolocation filters and clusters involved in the 'push' have been selected.

Click the **Push Config** button to 'push' (copy) a selected list of geolocation filters to a selected list of clusters. This allows the provider administrator to create the same geolocation filters on multiple clusters in a single step.

EMCC Parameters and Profile

The EMCC feature parameters are settings that need to be present and configured on the various clusters participating in the EMCC functionality. The Intercluster Service profile determines how communication between clusters participating in the EMCC functionality will be handled.

The *EMCC Parameters* screen allows the configuration of the Extension Mobility Cross Cluster (EMCC) feature parameters as well as the intercluster service profile.

Note

Only provider administrators are able to manage the EMCC parameters and intercluster service profile settings, and only if a geolocation filter is already configured.

Procedure

- Step 1** Browse to *Network > PBX Devices* .

- Step 2** Select the required CCM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.
- Step 5** Click the **EMCC Parameters and Profile** button. The *EMCC Parameters* screen is displayed.
- Step 6** Complete the required fields (see table below for field descriptions):

Parameter	Description
EMCC Parameters	
Default TFTP Server for EMCC Login Device	Select the computer name or IP address from the drop-down list of the default TFTP server that should be used by devices logging into EMCC from a remote cluster. Until a selection is made, this cluster will not be able to support EMCC.
Backup TFTP Server for EMCC Login Device	Select the computer name or IP address from the drop-down list of the backup TFTP server that should be used by devices logging into EMCC from a remote cluster. If the default TFTP server fails or becomes unavailable or unresponsive, and a backup TFTP server has not been defined, then EMCC will fail.
Default Interval for Expired EMCC Device Maintenance	Specify the number of minutes that will elapse between checks of the system for expired EMCC devices. An expired EMCC device is a device that has logged into the EMCC service from a remote cluster, but due to WAN failure or connectivity problems, has logged out of the home cluster, and when connectivity was restored, logged back into the home cluster. During this maintenance job, the Cisco Extension Mobility service checks the Cisco Unified Communications Manager (Unified CM) database for any expired EMCC devices and automatically logs them out. This is a mandatory field. Default = 1440, Minimum = 10, Maximum = 1440.
Enable All Remote Cluster Services When Adding A New Remote Cluster	Valid values include; True (enable all services on the remote cluster automatically) or False (manually enable the services on the remote cluster via the Remote Cluster Configuration window in Unified CM Administration). It may be preferable to enable the services manually to allow time to configure the EMCC feature completely before enabling the remote services. This is a mandatory field. Default = False.
CSS for PSTN Access SIP Trunk	Select the Calling Search Space (CSS) from the drop-down list that will be used by the PSTN access SIP trunk for processing EMCC calls. The PSTN access SIP trunk is the SIP trunk that has been configured for PSTN access in the Intercluster Service Profile window in Unified CM Administration. Calls over this trunk will only be routed to the local PSTN that is co-located with the EMCC logged in phone initiating the call. Valid values specify Use Trunk CSS (PSTN calls will utilize the local route group which can be useful for properly routing emergency service calls) or Use Phone's Original Device CSS (PSTN calls will be routed using the configured calling search space on the remote phone; that is, the CSS that is used when the phone is not logged into EMCC). This is a mandatory field. Default = Use trunk CSS.

Parameter	Description
EMCC Geolocation Filter	<p>Select the required geolocation filter from the drop-down list that has been configured for use with the extension mobility cross-cluster feature. The EMCC geolocation filters must have been previously configured in order to select it from this drop-down list. Depending on the information in the geolocation that is associated with a phone logged in via extension mobility from another cluster, and the selected EMCC geolocation filter, Unified CM will place the phone into a roaming device pool.</p> <p>Note</p> <p>If this parameter is set to <i>None</i>, EMCC will not function correctly; phones that attempt to login but cannot be assigned to a roaming device pool will fail to login.</p>
EMCC Region Max Audio Bit Rate	<p>Select the maximum audio bit rate for all EMCC calls from the drop-down list, regardless of the region associated with the other party.</p> <p>Note</p> <p>All participating EMCC clusters must specify the same EMCC Region Max Audio Bit Rate. This is a mandatory field. Default = 8 kbps (G.729).</p>
EMCC Region Max Video Call Bit Rate (Includes Audio)	<p>Enter the maximum video call bit rate for all EMCC video calls, regardless of the maximum video call bit rate of the region associated with the other party.</p> <p>Note</p> <p>All participating EMCC clusters must specify the same EMCC Region Max Video Call Bit Rate. This is a mandatory field. Default = 384, Minimum = 0, Maximum = 8128.</p>

Parameter	Description
EMCC Region Link Loss Type	<p>Select the link loss type between any EMCC phone and devices in any remote cluster from the drop-down list.</p> <p>Note</p> <p>All participating EMCC clusters must use the same EMCC Region Link Loss Type. Based on the option chosen, Unified CM will attempt to use the optimal audio codec for the EMCC calls, while observing the configured EMCC Region Max Audio Bit Rate. Valid values specify Lossy (where some packet loss can or may occur, for example, DSL) or Low Loss (where low packet loss occurs, for example, T1). When this parameter is set to Lossy, Unified CM chooses the optimal codec within the limit set by the EMCC Region Max Audio Bit Rate. This is based on audio quality, given the assumption that there will be some packet loss. When this parameter is set to Low Loss, Unified CM chooses the optimal codec within the limit set by the EMCC Region Max Audio Bit Rate, based on audio quality, given the assumption that there will be little or no packet loss. The only difference in the ordering between the Low Loss and Lossy options is that G.722 is preferred over iSAC (Internet Speech Audio Codec) when the Link Loss Type is set as Low Loss, while iSAC is preferred over G.722 when the Link Loss Type is set as Lossy. This is a mandatory field. Default = Low Loss.</p>
RSVP SIP Trunk Keep-Alive Timer	<p>Enter the number of seconds that Unified CM should wait between sending or receiving KeepAlive messages or acknowledgments between two clusters over EMCC RSVP SIP trunks. An EMCC RSVP SIP trunk has EMCC configured as the trunk service type and has been selected as the SIP trunk for the RSVP agent in the Intercluster Service Profile window. When two of these intervals have elapsed without a KeepAlive or an acknowledgment, it is assumed that there are no roaming users currently logged in (all active users have logged off), and Unified CM releases the RSVP resources with the remote cluster.</p> <p>This is a mandatory field. Default: 15, Minimum: 1, Maximum: 600.</p>
Default Server For Remote Cluster Update	Select the default server name or IP address from the drop-down list of the primary Unified CM server in this local cluster where extension mobility has been activated. The remote cluster will access this server to get information about this local cluster.
Backup Server for Remote Cluster Update	Select the default server name or IP address from the drop-down list of the secondary Unified CM server in this local cluster that has the extension mobility service activated. The remote cluster will access this server when the primary server is down to get information about this local cluster.
Remote Cluster Update Interval	<p>Enter an interval, in minutes, that the extension mobility service on the local Unified CM node should collect information about the remote EMCC cluster. Collected information includes such details as the remote cluster Unified CM version, service information, and so on.</p> <p>This is a mandatory field. Default = 30, Minimum = 15.</p>
Intercluster Service Profile	

Parameter	Description
EMCC Active	Select this checkbox to activate the Cisco Extension Mobility Cross Cluster feature. EMCC will not work if this is not switched ON.
PSTN Active	Select this checkbox to activate PSTN access.
RSVP Agent Active	Select this checkbox to activate RSVP Agent.
Use PSTN Access SIP Trunk for RSVP Agent	Select this checkbox to use the same SIP Trunk for RSVP Agent as is used for PSTN Access.

Step 7 Click the **Modify** button when complete. The parameters will be modified in the database.

Roaming Device Pool Management

A roaming device pool gets assigned to a device/phone from the home cluster once an EMCC user has logged in at the visiting cluster. The specific device pool that gets assigned is determined by matching the geolocation of the device/phone to the geolocation of the roaming device pool as per the geolocation filter selected in the EMCC Parameters on the home cluster.

The *Roaming Device Pool Management* screen allows administrators to view/modify existing roaming device pools in the cluster, add new roaming device pools to the cluster (see [To add or modify roaming device pools on page 411](#)), or to delete one or more existing roaming device pools from the cluster. Roaming device pools can also be 'pushed' (copied) to other clusters (see below).

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required Unified CM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **Home Cluster Setup** button. The *EMCC Home Cluster Setup* screen is displayed.
- Step 5** Click the **Roaming Device Pools** button. The *Roaming Device Pool Management* screen is displayed.

Delete a roaming device pool if required by selecting the checkbox adjacent to the relevant roaming device pool/s, and then clicking the **Delete** button. Click the *Select All* or *Select None* links (active text links) as required to select or deselect multiple roaming device pools.

Push config (roaming device pools)

Note

The **Push Config** button is inactive until both the roaming device pools and clusters involved in the 'push' have been selected.

Click the **Push Config** button to 'push' (copy) a selected list of roaming device pools to a selected list of clusters. This allows the provider administrator to create the same roaming device pools on multiple clusters in a single step.

To add or modify roaming device pools

Procedure

To add roaming device pools

- Step 1** Click the **Add** button on the *Roaming Device Pool Management* screen. The *Add Roaming Device Pool* screen is displayed.
- Step 2** Complete the required field (see table below for field descriptions):

Field	Description	Remarks
Device Pool Name	The name of the roaming device pool.	This is a mandatory field, and can only be modified during the <i>Add</i> process.
Adjunct Calling Search Space (CSS)	This field is used when extension mobility cross cluster is deployed, and is used to ensure that the country specific emergency dialing in the visiting cluster is supported.	Select the required adjunct CSS from the drop-down list.
Local Route Group	The local route group.	Select from the drop-down list. This is a mandatory field, and can only be modified during the <i>Add</i> process.
Geolocation	The geolocation.	Select from the drop-down list.

- Step 3** Click the **Add** button when complete to add the roaming device pool.
-

Procedure

To modify roaming device pools

- Step 1** Select the relevant roaming device pool name *link* (active text link) on the *Roaming Device Pool Management* screen.
- Step 2** Modify the required parameters in the fields provided (see table above for details).
- Step 3** Click the **Modify** button when complete. The roaming device pool parameters are modified in the database.
- Step 4** Click the **Delete** button **only** to delete the selected roaming device pool.
-

View EMCC Configuration

The *View EMCC Configuration* screen shows the existing configuration for the home cluster.

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required Unified CM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **View EMCC Configuration** button. The *View EMCC Configuration* screen is displayed.
-

The following configuration items are listed:

- EMCC Cluster
- Geolocation/s
- Geolocation Filter/s
- EMCC Trunks
- Roaming Device Pools
- Dial Plan
- EMCC Countries

Note

To view the detailed EMCC dial plan configuration, click the *View EMCC Dial Plan Configuration* link (active text link).

There is also an option to export a report of the configuration to an xml file by clicking the **Report Export** button. Other clusters can then use the parameters listed in the report to make sure that EMCC is configured correctly between their cluster and the cluster the report was run from. Additional manual configuration around server certificates, etc. is required to ensure that the EMCC feature functions between the different clusters. This is typically used when the participating clusters are owned and managed by different service providers.

EMCC Group Management

An Extension Mobility Cross Cluster (EMCC) group is a collection of clusters and countries that essentially forms an 'EMCC Cloud', which determines the specific clusters between which a user can roam.

EMCC groups typically cater for situations where all the clusters are in different countries, and are managed by the same platform instance. To support multiple clusters in the same country, you need to refine the geolocations and geolocation filters to uniquely identify the clusters in the default provisioning of country. This is supported by using the home cluster setup for each of the clusters in the group.

The *EMCC Group Management* screen allows a provider administrator to add or remove clusters and countries to an EMCC group, or to modify/delete an existing EMCC Group.

Note

A cluster can be included in multiple groups, but the same two clusters may not be included in more than one EMCC Group at the same time.

EMCC Group Setup

When adding an EMCC Group, the cluster the user is on when taking this action is automatically selected/included in the new group. Add an EMCC Group as follows:

Procedure

Adding an EMCC Group

- Step 1** Browse to *Network > PBX Devices*.

- Step 2** Select the required CCM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **EMCC Group Setup** button. The *EMCC Group Management* screen is displayed.
- Step 5** Click the **Add** button. The *EMCC Group Setup* screen is displayed.
- Step 6** Enter the *EMCC Group Name* and *Description* in the *EMCC Group Management* area of the screen.
- Step 7** Add the required EMCC Clusters and EMCC Countries to the selected EMCC Group by moving single or multiple entries into the relevant list boxes. Use the **Select All**, **Add>>**, **<<Remove**, **All>>**, etc. buttons as required.
- Step 8** Make sure that the required EMCC Clusters and Countries are listed in the *Selected EMCC Clusters* and *Selected EMCC Countries* areas of the screen respectively.
- Step 9** Click the **Apply EMCC Group Configuration** button when complete. The EMCC group is added to the database.
-

Procedure

Modifying an EMCC Group

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required CCM server *link* (active text link).
- Step 3** Click the **EMCC** button. This button is only visible if the server is EMCC enabled (see previous section).
- Step 4** Click the **EMCC Group Setup** button. The *EMCC Group Management* screen is displayed.
- Step 5** Select the relevant EMCC Group *link* (active text link). The *EMCC Group Setup* screen is displayed.
- Step 6** Enter or verify the *EMCC Group Name* and *Description* in the *EMCC Group Management* area of the screen.
- Step 7** Add or remove the required EMCC Clusters and EMCC Countries to/from the selected EMCC Group by moving single or multiple entries to/from the relevant list boxes. Use the **Select All**, **Add>>**, **<<Remove**, **All>>**, etc. buttons as required.
- Step 8** Make sure that the required EMCC Clusters and Countries are listed in the *Selected EMCC Clusters* and *Selected EMCC Countries* areas of the screen respectively.
- Step 9** Click the **Apply EMCC Group Configuration** button when complete. The EMCC group is modified in the database.
- Step 10** Click the **Delete** button **only** to delete the selected EMCC group.
-

Note

An EMCC Group can not be deleted if there are users enabled for Extension Mobility Cross Cluster on any of the clusters in the EMCC Group.

To delete an EMCC Group, select the checkbox adjacent to the EMCC Group(s) to delete on the *EMCC Group Management* screen, and then click the **Delete** button to delete the selected

EMCC Group(s). Delete an individual EMCC group (if required) as described in the last step of the previous section.

Enabling/Disabling EMCC using the Bulk Loaders

EMCC can be enabled/disabled for users by modifying the *EMCC Enabled* setting on the *Add or Modify User Mobility* sheet in the *LocAdmin* spreadsheet, True=Enabled and False=Disabled.

Refer to the Bulk Loader Guide for more information if required.

Extension Mobility Location Group Management

Overview

Extension mobility location groups are created to provide an additional level of restriction for extension mobility. This restriction is based on the location of the user as well as the location of the phone the user attempts to log in to.

To manage this, a Customer administrator (or higher) can create extension mobility location groups, which consist of selected customer locations. An end user can then use their mobility profile to log into phones assigned to locations in the **same** extension mobility location group as the location at which the user is provisioned.

Note

The Provider level preference *BVSMUserRoaming* **must be enabled** for this feature to work.

Important points to remember/restrictions

- A location can only belong to **one** extension mobility location group.
- Users at a location that is not assigned to an extension mobility location group can use phones at any location under their customer as normal.
- Users at locations assigned to Group A will not be able to log into phones at locations assigned to Group B, and visa-versa.

Procedure

To access extension mobility location groups:

- | | |
|---------------|--|
| Step 1 | Browse to <i>General Administration > Extension Mobility Location Groups</i> . The <i>Extension Mobility Location Groups</i> screen is displayed. |
| Step 2 | View the existing extension mobility location groups, which provide the extension mobility group <i>Name</i> and <i>Description</i> . |
-

The *Extension Mobility Location Groups* screen displays all currently configured extension mobility location groups.

Existing extension mobility location groups can be modified by selecting the relevant extension mobility location groups *Name* (active text link).

New extension mobility location groups can be created by clicking the **Add** button.

A search facility is available to search for a specific extension mobility location group by entering the relevant search criteria, and then clicking the **Search** button.

Existing extension mobility location groups can be deleted by clicking the **Delete** button adjacent to the relevant extension mobility location groups name.

Multiple extension mobility location groups can be selected and deleted (if required) by selecting the appropriate checkboxes and/or clicking the relevant **Select All**, **Select None**, and **Delete Selected** buttons.

Adding an Extension Mobility Location Group

A Customer administrator (or higher) can create extension mobility location groups.

Procedure

To add an extension mobility location group:

- Step 1** Click the **Add** button on the *Extension Mobility Location Groups* screen. The *Add Extension Mobility Location Group* screen is displayed
 - Step 2** Complete all the required fields (see table below for field descriptions).
 - Step 3** Click the **Add** button when complete to add the extension mobility location group.
-

Available extension mobility location group fields include:

Field	Description	Remarks
Name	The name for the extension mobility location group.	This is a mandatory field.
Description	A brief description of this extension mobility location group.	-
Associated Locations	Add or remove locations to/from this extension mobility location group by selecting the relevant location(s) in the <i>Available</i> area of the screen and then clicking the Add>> button, or by selecting the relevant location(s) in the <i>Selected</i> area of the screen, and then clicking the << Remove button. Use the <i>Select All</i> link(s) (active text links) to select multiple locations if required.	-

Modifying an Extension Mobility Location Group

Procedure

To modify an extension mobility location group:

- Step 1** Select the required extension mobility location group *Name* (active text link) that you want to modify on the *Extension Mobility Location Groups* screen.
 - Step 2** Update the required fields, and then click the **Modify** button. Refer to the table under [Adding an Extension Mobility Location Group on page 416](#) for details on each field if required.
-

Note

The displayed extension mobility location group can also be deleted by clicking the **Delete** button on this screen.

Mobile Connect/Single Number Reach (SNR)

Mobile Connect (Single Number Reach) enables an incoming call to a corporate phone to be directed to the user's normal desk phone as well as up to ten other configurable destinations. The remote destinations would usually be a mobile (cellular) phone or a user's home phone number. Once the call has been directed to the desktop and remote phone(s), the user can answer either device. Upon answering the call, the user can transfer the call to one of the other devices.

In order for a user in a location to have SNR, the feature should be enabled for the user (via the feature group) and the location. The SNR button appears for a user if it is in their feature group, however they receive an error message if the location is not enabled for SNR (*This location does not support single number reach*).

Note

- The SNR Name and Number are unique per Cisco Unified Communications Manager (Unified CM) Cluster.
 - Even if single number reach has been activated in a Feature Group, an error message is still received if the location has not been enabled for single number reach.
 - Certain phones do not support SNR, make sure that phones are placed in feature groups where the settings are off for the features the phone doesn't support.
 - The remote destination profile name in Unified CM is derived from the username in CUCDM, and then appended with '-rdp'. If the CUCDM username contains one of the following characters, / \ [] { } () " ' , : or @ then each of these characters is replaced by an underscore '_' character, and the remote destination profile name is appended with the userid to make sure that it is unique.
-

Enable Single Number Reach functionality for the User

SNR is managed at a user level and is a feature managed via Feature Groups, namely *Single Number Reach / Mobile Connect* under the *Value Add* section. From the main menu, browse to *General Administration > Feature Groups*, select the customer, Feature Group, enable (checkbox) the feature and click the **Modify** button.

Enable Single Number Reach functionality for a Location

SNR needs to be enabled for a location by checking the *Single Number Reach Support* checkbox on the relevant *Location Management* screen. This can be done during AddLocation or when modifying a location to enable SNR for the location.

When this is enabled during AddLocation the additional model CCM model call of AddSNR is made. When modifying a Location, the AddSNR or DelSNR CCM model call is made depending on what the setting was changed to.

Single Number Reach Calling Search Space

To use PSTN destinations as a SNR Remote Destination, a Rerouting CSS needs to be configured, that has access to the specified destination (Home Phone, Mobile Phone, etc.)

SNR Rerouting can be configured by means of the following:

- With COS-per-profile disabled at the customer level (default setting), the SNR rerouting COS can be controlled via values set per location and per customer - see [Advanced Telephony](#)

[Management on page 771](#) and [Advanced Telephony Settings on page 704](#) for more details if required. The existing dialplan default CSS is still applied if these values have not been set.

- With COS-per-profile enabled for a customer, the COS value can be individually configured for each SNR profile (i.e. each end user) - see [Adding a Single Number Reach Remote Destination on page 418](#) for more details if required.

In order to display the *A-Number* correctly on the Remote Destination, a Transformation CSS also needs to be defined, along with the appropriate Transformation Patterns. Both of these can be set in the CCM Models Loader, under the *Setup Tools/ Global Settings* menu option.

The impact of switching between the two modes is as follows:

- Enabling CoS per Profile - When COS-per-profile is switched on (enabled), the current effective COS value of each existing SNR profile, that is location default or customer default, is 'frozen' for that profile to make it independent of the default values. This involves updating the CUCDM database but not the Unified CM, as the effective value is not being changed.

Because the dial plan global setting is a CSS value, not a COS, this value for each SNR profile cannot be stored. Therefore, COS-per-profile cannot be enabled when the customer has any existing SNR profiles that are using the dial plan default value, that is, are not subject to a location or customer default COS value. For this reason, a default rerouting COS for the customer must be set before the COS-per-profile setting becomes available.

- Disabling CoS per Profile - When COS-per-profile is disabled, all SNR profiles are reset to the applicable default value (location, customer or dial plan). This involves updating the CUCDM database, as well as reprovisioning the profiles on the Unified CM.

Note

This operation cannot be reversed, as the individual COS settings for each profile are lost during this process.

Adding a Single Number Reach Remote Destination

To add a SNR remote destination, browse to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the *User Management* screen, click the **Single Number Reach** button.

Enter a Name, Description, Number and select extensions (if available). There are two options with checkboxes which can be selected per Remote Destination: *Mobile Phone*, and *Enable Mobile Connect*. Select *Either*, *None* or *Both*, and click the **Add** button.

Note

- The SNR name and number must be unique per Unified CM Cluster.
 - Destinations cannot be associated with a line that is auto-answer-enabled. Extensions that have auto-answer enabled are not available for selection and if auto answer is activated after a line has been enabled for SNR, the transaction fails.
 - A remote destination cannot be created without associating an extension to it.
 - The remote destination profile name in Unified CM is derived from the username in CUCDM, and then appended with '-rdp'. If the CUCDM username contains one of the following characters, / \ [] { } () " ' , : or @ then each of these characters is replaced by an underscore '_' character, and the remote destination profile name is appended with the userid to make sure that it is unique.
-

Fields available when adding a single number reach include:

Field	Notes	Remarks
User Details		
Username	The name of the user who's Single Number Reach is being managed.	This field is for information purposes only and cannot be modified here.
Feature Group	The feature group associated with the selected user.	This field is for information purposes only and cannot be modified here.
Profile Description	A brief description of the single number reach profile.	-
Device Pool	The device pool associated with the selected user.	All device pools available at the location are displayed in this list.
Primary Device	When using the SNR functionality, users have to select a primary device from the drop-down list.	<p>Available primary devices include devices associated to the end user and extensions that exist at existing remote destinations.</p> <p>Note</p> <p>Unified CM 9.1.1 and later no longer support this functionality, and in these instances, it is best practice to set this drop-down option to <i>None</i>.</p> <p>See Setting and Resetting a Primary Device for an End User on page 424 for more information if required.</p>
Privacy	When privacy is enabled (select <i>On</i>), the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled (select <i>Off</i>), the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls.	-
Rerouting CoS	Sets the re-routing CoS to be used for this specific SNR profile. Select the required CoS value from the drop-down list. Available values are the 'outbound' service types configured for the dialplan.	<p>Note</p> <p>This field is only available if the <i>Allow CoS per SNR Profile</i> setting is enabled for the relevant Customer (see Advanced Telephony Settings on page 704).</p>
User Single Number Reach Settings		

Field	Notes	Remarks
Mobile Phone	Selecting the <i>Mobile Phone</i> checkbox gives a user the ability to "hand off" an active desk phone call to the desired Remote Destination, by pressing the <i>Mobility</i> softkey. Once the Remote Destination answers, the desk phone releases the call.	Note The Mobility softkey needs to be added to the device's softkey template in order for this feature to work.
Enable Mobile Connect	Selecting the <i>Enable Mobile Connect</i> checkbox enables both the desk phone, as well as the Remote Destination, to ring for incoming calls.	If this checkbox is selected you can also configure a ring schedule as required (see <i>Ring Schedule</i> field below for details).
Enable Fixed Mobile Convergence (FMC)	Selecting the <i>Enable Fixed Mobile Convergence</i> checkbox results in your desk phone number being displayed to the called party when making a call from your mobile device associated to your remote destination (Single Number Reach) profile.	If this checkbox is selected, the country code drop-down for the remote number is available (for HCS Provider only), and the <i>FMC Primary</i> radio button selection is available (see <i>Select from available lines / Available extensions to user</i> field below). Note The <i>Mobile Phone</i> checkbox (see above) must be selected before the Fixed Mobile Convergence (FMC) feature is available.
Remote name	The name of the single number reach.	This is a mandatory field and must be a unique name within the system.
Privacy	When privacy is enabled (select <i>On</i>), the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled (select <i>Off</i>), the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls.	-
Description	A short description of the single number reach entry.	-
Rerouting CoS	Sets the re-routing COS to be used for this specific SNR profile. Select the required Cos value from the drop-down list. Available values are the 'outbound' service types configured for the dialplan.	Note This field is only available if the <i>Allow CoS per SNR Profile</i> setting is enabled for the relevant Customer (see Advanced Telephony Settings on page 704).

Field	Notes	Remarks
Remote number	The number or URI to which the call must re-direct. This is a mandatory field.	<p>This must be the complete number or URI that must be dialed and is typically in the format that you would dial from your phone.</p> <p>Note</p> <p>A URI is in the username@host format, where the host can be an IPv4 address or fully qualified domain name. The username portion of a URI can be a maximum of 47 characters and the full URI a maximum of 254 characters.</p> <p>If a country is selected from the drop-down list, then only the required number must be entered. The countries displayed in the drop-down list are those available to the provider. The drop-down list provides for easier configuration.</p> <p>If <i>None</i> is selected, then the complete number that the call must be re-directed to must be entered (this includes a '+' sign, followed by the country code, followed by the actual number). Valid characters for this field are '+' (used only when entering the country code manually) as well as the numbers 0-9. Note that the '+' and '#' characters are not valid URI characters.</p> <p>Contact your administrator if required for more details of the number to be configured, or if you experience trouble with SNR ringing the remote destination.</p>
Answer too late timer	When selected, the system disconnects the remote destination if it is not answered within the specified time frame. It is best to ensure that this time frame is under the length of time it takes for the remote device to send the call to voicemail.	<p>Note</p> <p>This is a mandatory field, and is specified in milliseconds.</p> <p>The default value is 19000. This field must be supplied as either 0, or within the range of 10000 to 300000.</p>

Field	Notes	Remarks
Answer too soon timer	When selected, the system disconnects the remote destination if it is answered within the specified time frame. This is used mainly to detect when a remote device has answered and directed the call straight to voicemail.	<p>Note</p> <p>This is a mandatory field and is specified in milliseconds.</p> <p>The default value is 1500. This field must be supplied as a numeral within the range of 0 to 10000.</p>
Delay before ringing timer	This setting is used to delay the ringing of the remote destination phone. This is used to further lengthen the amount of time that must pass before a remote destination phone forwards the call to its own voicemail box.	<p>Note</p> <p>This is a mandatory field and is specified in milliseconds.</p> <p>The default value is 4000. This field must be supplied as a numeral within the range of 0 to 30000.</p>
Select from available lines / Available extensions to user	This section lists all extensions available to the user. Select the checkbox adjacent to the line(s) that you would like to associate this SNR entry with.	<p>Note</p> <p>It is mandatory to select at least one extension when adding a remote destination.</p> <p>If you selected the <i>Fixed Mobile Convergence (FMC)</i> checkbox (see field above) then you can select the required <i>FMC Primary</i> radio button adjacent to the selected line. This selection determines the actual number displayed to the called party. Only one radio button can be selected, and only if the extension has been selected for SNR.</p>

Field	Notes	Remarks
Ring Schedule	This section allows users and administrators to set a ring schedule for remote destinations that have the mobile connect feature enabled (see <i>Enable Mobile Connect</i> field above).	<p>If you want to direct calls to the selected numbers at all times for a particular day, select the relevant checkbox next to the required day and leave the start and end times as 00:00.</p> <p>If you want to direct calls to the selected numbers only within certain start and end times for a particular day, select the relevant day checkbox and then select the required start and end times from the appropriate drop-down lists.</p> <p>Note</p> <p>The times shown in these fields automatically reflect the times as they are in the timezone for the country/area in which the end user is located, i.e. the end user's location.</p>

Feature Limitations/Exceptions

When associating an extension with more than one Remote Destinations, selecting the *Enable Mobile Connect* option does not ring all the Remote Destinations. Only the first one that was added and associated for a particular extension.

When associating an extension with more than one Remote Destinations, selecting the *Mobile Phone* does not give the user the option of handing the call off to all the Remote Destinations. Only the first one that was added and associated for a particular extension.

The *Mobile Phone* feature is limited only to users with roaming profiles/extension mobility.

Configuring SNR not to Interfere with Voicemail Boxes

To prevent a user from receiving work related voicemails in multiple mailboxes, the system enables administrators to configure SNR in a manner that ensures voicemail related to SNR sourced calls are always received in corporate mail box.

This is achieved by configuring timers to ensure that when a call is forwarded to a voicemail box on ring-no-answer, the call is forwarded to the enterprise voicemail box, this is achieved using two settings:

Forward-no-answer time: To do this, ensure the *forward-no-answer time* is shorter at the corporate desk phone than at the remote destination phone(s).

To do this, ensure that the global *Forward No Answer Timer* field in Unified CM or the No Answer Ring Duration field under the individual phone line is configured with a value that is less than the amount of time a remote destination phone rings before forwarding to the remote destination voicemail box.

In addition, the *Delay Before Ringing Timer* field can be used to delay the ringing of the remote destination phone in order to further lengthen the amount of time that must pass before a remote destination phone forwards to its own voicemail box.

Note

When adjusting the *Delay Before Ringing Timer* parameter, take care to ensure that the global Unified CM *Forward No Answer Timer* (or the line-level No Answer Ringer Duration field) is set sufficiently high enough so that the mobility user has time to answer the call on the remote destination phone.

Answer Too Late Timer: To do this, you need to ensure that the remote destination phone ceases ringing before it is forwarded to its own voicemail box. This is done by configuring the *Answer Too Late Timer* field to a value that is less than the time that a remote destination phone rings before it goes to voicemail. This ensures that the remote destination phone stops ringing before the call can be forwarded to its own voicemail box.

Answer Too Soon Timer: To ensure that a call is still forwarded to the corporate voicemail mailbox when a user's remote destination phone is busy or not available, you use the *Answer Too Soon Timer* field. Then, if a call is forwarded and answered immediately by the remote voicemail, this field ensures that the call is disconnected and allows for additional time for the desk phone to be answered or for the corporate voicemail system to answer the call.

Setting and Resetting a Primary Device for an End User

When provisioning SNR for a phone that is associated to an end user, the phone's Mobile Connect feature is not turned on when the user is not logged in to Extension Mobility. To address the issue, users are able to select a primary device for SNR.

Note

- The setting is configured per user and not per remote destination.
 - At least one remote destination must exist for an end user before the primary device can be set.
 - Only primary devices that are associated to the end user and to extensions that exist at existing remote destinations for the end user are listed as available choices.
 - Once set, the Enable Mobility setting for the phone is disabled on the Unified CM, the Owner User ID setting is set to the name of the user and the Primary Device is set to the name of the primary device chosen against the user on the Unified CM.
 - Extension Mobility is disabled for devices that are specified as primary devices. Users are not able to login to primary devices and all of the devices settings related to extension mobility, for example, the Allow user to login to phone setting, is disabled.
-

Resetting a Primary Device for an End User

At least one remote destination must exist for an end user before the primary device can be reset.

The drop-down list captioned *Primary Device* is used for resetting the primary device for the user. The option *None* must be selected for this purpose. Once reset, the *Enable Mobility* setting for the phone is enabled on the Unified CM, the *Owner User ID* setting is unset and the *Primary Device* is blanked against the user on the Unified CM.

Impact on the Phone Management Page

To remind users that *Extension Mobility* is disabled for a device chosen as primary device for SNR for a user, the phone management page on the system GUI displays a message *Extension Mobility disabled as this is the primary SNR device for user [username]*.

Modifying a Single Number Reach Remote Destination

Browse to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the *User Management* screen, click the **Single Number Reach** button. One or more Remote Destinations are shown.

Note

- The SNR Name and Number are unique per Unified CM Cluster.
 - If there is no connectivity between the system and Unified CM, then an error message is displayed next to the *Enable Mobile Connect* field, informing you that these values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the screen. Click the **Sync with Call Manager** button to manually sync these values with when connectivity has been restored.
-

Update the required details and click the **Modify** button for the relevant SNR entry. You may modify the Destination Name and Destination Number, as long as it stays unique within the Unified CM Cluster.

Available details are the same as for the SNR Addition process.

Deleting a Single Number Reach (SNR) Remote Destination

Browse to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the *User Management* screen, click the **Single Number Reach** button. One or more *Remote Destinations* are shown. Select the required remote name (active text link), and then click the **Delete** button to delete the selected SNR remote destination.

Impact of Deleting a Remote Destination

If the last SNR remote destination that contains an extension associated to the primary device is deleted, the Primary Device of the user is implicitly reset.

Checking the CCM Data

When a Remote Destination is created for the first time, a Remote Destination Profile is created for the User. The format of this is: *USERNAME-RDP*, for example, *7001001-RDP*.

Procedure

To verify that this is correct:

- Step 1** Login to the Unified CM.
 - Step 2** Browse to *Device > Device Settings > Remote Destination Profile*.
 - Step 3** Click the **Find** button.
-

Mobile Identity Management

Mobile Identity enables an incoming call to be directed directly to a remote destination, which in this instance is a mobile (cellular) phone.

Note

- Mobile Identity is only available in locations which are enabled for Single Number Reach.
- At least one Dual-mode phone must be assigned to the end user. For the Mobile Identity feature to work with the *Cisco Dual Mode for Android* phone type, the *Enable Cisco Unified Mobile Communicator* checkbox **must be selected** (enabled) in Unified CM.

Configuring Mobility Identity is very similar to configuring Single Number Reach as described under [Mobile Connect/Single Number Reach \(SNR\) on page 417](#).

Procedure**Activating Mobile Identity**

- Step 1** Browse to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the User Management screen, click the **Mobile Identity** button. The *Mobile Identity* screen is displayed.
- Step 2** Complete the required fields (see table below)
- Step 3** Click the **Add** button.

Field	Notes	Remarks
User Details		
Username	The name of the user who's mobility identity is being managed.	This field is for information purposes only and cannot be modified here.
Feature Group	The feature group associated with the selected user.	This field is for information purposes only and cannot be modified here.
Dual Mode Phone	The dual mode device associated with the Mobile Identity functionality.	Select from the drop-down list. Note For the Mobile Identity feature to work with the <i>Cisco Dual Mode for Android</i> phone type, the <i>Enable Cisco Unified Mobile Communicator</i> checkbox must be selected (enabled) in Unified CM.
Mobile Identity Settings		
Remote Name	The name of the mobility identity entry.	This is a mandatory field, and must be a unique name within the system.
Description	A short description to identify the mobile identity entry.	Modify description as required.

Field	Notes	Remarks
Remote number	The number that the call will be re-directed to. This is a mandatory field.	<p>This must be the complete number that must be dialed and is typically in the format that you would dial from your phone.</p> <p>If a country is selected from the drop-down list, then only the required number must be entered. The countries displayed in the drop-down list are those available to the provider. The drop-down list provides for easier configuration.</p> <p>If <i>None</i> is selected, then the complete number that the call must be re-directed to must be entered (this includes a '+' sign, followed by the country code, followed by the actual number). Valid characters for this field are '+' (used only when entering the country code manually) as well as the numbers 0-9.</p> <p>Contact your administrator if required for more details of the number to be configured, or if you experience trouble with mobile identity ringing the remote destination.</p>
Mobile Phone	The Mobile Phone checkbox.	Checkbox enabled by default when the Mobile Identity feature is enabled for an end user.
Enable Mobile Connect	Selecting this checkbox allows the device to ring for incoming calls when used as a desk phone.	-
Enable Fixed Mobile Convergence	Selecting the Enable Fixed Mobile Convergence checkbox results in your desk phone number being displayed to the called party when making a call from your mobile device associated to your remote destination profile.	-
Answer too late timer	When selected, the system will disconnect the remote destination if it is not answered within the specified time frame.	<p>Note</p> <p>This is a mandatory field and is specified in milliseconds.</p> <p>The default value is 19000. This field must be supplied as either 0, or within the range of 10000 to 300000.</p> <p>It is best to ensure that this time frame is under the length of time it will take for the remote device to send the call to voicemail.</p>

Field	Notes	Remarks
Answer too soon timer	<p>When selected, the system will disconnect the remote destination if it is answered within the specified time frame.</p> <p>This is used mainly to detect when a remote device has answered and directed the call straight to voice-mail.</p>	<p>Note</p> <p>This is a mandatory field and is specified in milliseconds.</p> <p>The default value is 1500. This field must be supplied as a numeral within the range of 0 to 10000.</p>
Delay before ringing timer	<p>This setting is used to delay the ringing of the remote destination phone. This is used to further lengthen the amount of time that must pass before a remote destination phone will forward the call to its own voicemail box.</p>	<p>Note</p> <p>This is a mandatory field and is specified in milliseconds.</p> <p>The default value is 4000. This field must be supplied as a numeral within the range of 0 to 30000</p>
Available Phone Extensions	<p>This is used to select the primary FMC extension.</p>	<p>Select the radio button next to the required extension number (line).</p>

Procedure

Modifying a Mobile Identity Entry

- Step 1** Browse to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the User Management screen, click the **Mobile Identity** button.

Note

If there is no connectivity between the system and Cisco Unified Communications Manager (Unified CM), then an error message is displayed next to the *Enable Mobile Connect* field, informing you that these values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the page. Click the **Sync with Call Manager** button to manually sync these values with the Unified CM when connectivity has been restored.

- Step 2** Select the relevant *Remote name* (active text link) mobile identity entry to update.
- Step 3** Update the required details (available fields are described in the above table) and click the **Modify** button.

Procedure

Deleting a Mobile Identity Entry

- Step 1** Navigate to *Location Administration > End Users*, navigate via the hierarchy (Provider, Reseller...) and select a user. On the User Management screen, click the **Mobile Identity** button.
- Step 2** Select the relevant *Remote name* (active text link) mobile identity entry to delete.
- Step 3** Click the **Delete** button to delete the selected mobile identity entry.

Synchronization with Cisco Unified Communications Manager (Unified CM)

If the system has connectivity with the Unified CM, the system simply retrieves certain settings from the Unified CM and displays in the relevant system GUI if they differ from those stored in the system database.

If there is no connectivity with Unified CM, the system displays a message next to the relevant setting *Call forward all calls to voicemail*, indicating "Unable to connect to Call Manager. Warning: these values may be out of Sync".

A **Sync with Call Manager** button also appears next to the **Modify** or **Apply** button (as appropriate) on the relevant screen. This button allows the user to attempt to connect to the Cisco Unified Communications Manager using a longer timeout of five (5) seconds as opposed to the default of one second and then resynchronize any values that are different. The *Call forward - always* field is synced in a similar manner to the *Call forward all calls to voicemail* field.

Note

The *Call forward - always* setting takes precedence over all other call forward settings, except *Call forward all calls to voicemail*.

The *Call forward all calls to voicemail* setting takes precedence over all other call forward settings.

The following features and settings in the Admin GUI as well as the Self Care GUI use this functionality:

Unified CM Setting	Associated System Interface
Call forward all calls to voice-mail	Manage Extension Mobility Profile
Call forward - always	Phone (Line Management) CTI Device Management
Enable Mobile Connect	Single Number Reach Mobile Identity

Subnets

An IP Subnet is a logical group of IP Addresses, normally based on the private address range within a Provider or Customer. The system allows a location to have multiple subnets and administrators can also share a single subnet between two different locations.

The system stores more information about managed subnets than unmanaged. This allows the system to ensure that elements of a managed subnet are used correctly in terms of networking. The system assumes that another server is controlling the elements of an unmanaged subnet.

Note

Each phone within the system must have a unique IP address. The system does not allow an operator to allocate incorrect IP Subnet addresses to a location.

The sections below provide an overview of subnets and related topics within the system.

NAT and PAT

Overview of NAT and PAT:

- **NAT (Network Address Translation)** is standard that enables a local area network (LAN) to use one set of IP addresses for internal network traffic and a second set of addresses for external traffic.
- **PAT (Port Address Translation)** is a form of network address translation whereby each IP Address on the LAN is translated to the same IP address but each with a different port.

The system supports both PAT and NAT based subnets. By default, subnets are added as NAT.

Note

The system only supports PAT with a 32 bit subnet.

Adding and Managing Subnets

These are voice subnets which the phones reside in. There are two types of subnets:

- **Managed:** These are subnets which the system provisions and manages on the DHCP server. This option should be used when the system provisions the DHCP server and handles IP address allocation for devices. This requires the DHCP messages for devices to be sent to the DHCP server (ip-helper setup in the network). Managed IP subnets are managed via the *Resources > Managed IP Subnets* menu option.
- **Unmanaged:** These are subnets which the system does not provision or manage. However the system knows about the subnets and provides AutoMove via Syslog integration with Unified CM. These subnets require some other DHCP service in the network to provide the DHCP functionality to the endpoints and the system is not involved. Unmanaged subnets are managed via the relevant *Location Management* screen accessed via the *General Administration > Locations* menu option.

When adding and managing managed subnets within the system, the following are the key available fields:

- **DHCP server controlling this subnet:** This tells the system which DHCP server to provision for the subnet.
- **Origin IP of DHCP messages encapsulated by router:** See field description below.
- **Alternate Origin IP of DHCP messages (HSRP paired routers):** This setting, and the Origin IP of DHCP messages encapsulated by router setting above relate to the DHCP-based AutoMove capability in the system. These settings allow the system to map the source addresses of the DHCP requests to this subnet to identify the location to move to and subnet to allocate the address from. The alternate setting is in case the DHCP requests are not all from the same source address. One example is that in a network with IOS devices setup with HSRP as the default route, the DHCP requests are sourced with the physical interface of the IOS devices (typical the vlan interface address) instead of the virtual HSRP address. In this instance, both the Origin and Alternate Origin need to be configured: one with the IP address for device 1 and one with the IP address for device 2. The DHCP logs or DHCP packets on the network can be inspected to determine the source addresses if AutoMove is not working as expected.
- **Domain Name:** Added to the DHCP server configuration as the domain for the subnet. For unmanaged subnets, has no effect.
- **Primary DNS server IP:** Added as part of the subnet configuration in the DHCP server. No affect for unmanaged subnets.

- **Fallback DNS server IP:** Added as part of the subnet configuration in the DHCP server. No affect for unmanaged subnets.
- **IP address for default route of Phone:** This is relevant to the system managed subnets where the DHCP configuration requires this default gateway setting as part of the subnet definition. No affect for unmanaged subnets.

Edge Devices

When adding standard or shared building locations a subnet must be selected. Subnets are also managed at existing locations, and are added/modified via a drop-down list. For customers that use large amounts of subnets these dropdown may become too large, and may cause the Administrator to make an error. IP Edge Devices are used in these instances to limit the list of subnets available at building locations specifically. If an IP Edge Device is associated to a building, only subnets that are assigned to the same IP Edge Device are available to locations at the relevant building.

Extension Management

Every location in the system can have a number of internal numbers (extensions) assigned to it. The number of extensions allowed depends on the *extension digits* value of that location (normally 4 digits). A value of 4 will give a valid extension range of 0000-9999 and a value of 3, 000-999 etc.

Note

When a location is created, only the extensions that are needed are created.

Managing Available Internal Numbers

Procedure

Managing Internal Number Ranges Allocated to the Location

To manage extension ranges allocated to a location:

- Step 1** Browse to *Location Administration > Internal Numbers*
- Step 2** Select the **Extension Range Management** button
- Step 3** To delete a range, select the **Delete** button adjacent to the range that you would like to delete
- or

To allocate a range, select the **Add Extension Range** active text link adjacent to the required number range.

Procedure

Managing Internal Number Ranges

To manage extension ranges:

- Step 1** Browse to *Location Administration > Internal Numbers*
- Step 2** Select the **Extension Range Management** button

Extensions are managed using ranges:

a Option 1

Enter the start extension and the end extension number or range size, then select either the **Add** or **Delete Range** button.

or

b Option 2

Enter a list of start extension and end extension numbers in a range style. For example, 0000-0100, 0200-0299 etc, then select the **Add** or **Delete Range** button.

Note: Extensions (Internal Numbers) can be managed via the bulk loaders.

Manage Extensions (Internal Numbers) using Bulk Loaders

Extension numbers can be created when adding a location using the **Add** Locations sheet. Add valid extension ranges in the form extension-extension, extension-extension, for example, 0000-0100, 0200-0299. In the *Allowed Extension Ranges* column.

Connect Location

Connect Location is used primarily during roll-out and migration, and enables administrators to plan and prepare a location without actually provisioning the location. This is useful for scenarios where you are migrating a system from, for example, a TDM PBX to IP based and you would like to provision all of the phones, users, class of service, and so on ahead of time.

Traditionally, provisioning the entire dial plan ahead of time creates 'black-holes' within the network where calls do not route correctly. Connect location is a model driven approach that enables administrators to select and configure components without actually taking the location's configuration live. Once administrators are ready to take the location live, the Connect Location functionality completes the configuration and makes the relevant calls based on what is specified in the model.

Note

Although the Connect Location feature is managed via the CUCDM GUI, this feature relies closely on the bulk and model loaders. For information on the bulk and model loaders, refer to the *Model and Bulk Loader Guide Series*.

Via the *Location Administration* Menu

Procedure

To connect (activate) a location using the *Location Administration* menu:

Step 1 Browse to *Location Administration > Telephony > Telephony*.

Step 2 Click the **Connect** button adjacent to the relevant location.

Step 3 Enter the following parameters in the associated fields:

- Pattern (#CLOCPATTERN#) - This is a free-format text entry that replaces the #CLOCPATTERN# variable in the models. This field is available only if route patterns and/or translation patterns are found for model name/s matching the *ConnectLocation* name.
Caution: If the pattern entered here already exists in the same partition selected from the *ConnectLocation* model name suffix, then the existing pattern will be overwritten on the Unified

CM. This includes all calling/called transformation patterns, route patterns, translation patterns, hunt pilots and directory numbers.

- Model name suffix - Select from the drop-down list. This drop-down list contains the suffixes for all matching models. This field is available only if route patterns and/or translation patterns are found for model name/s matching the *ConnectLocation-* name. A *None* option is available in order to skip IPPBX provisioning. However make sure that there is no model name called *ConnectLocation-* (with a blank prefix), as CUCDM would then identify this as the model that you want to provision to the IPPBX.

Step 4 Click the **Connect** button to connect the selected location.

Click the **Disconnect** button if you want to disconnect the location.

Note

- If a site is already connected, the **Connect** button is not available in the GUI as a connected location cannot be connected again.
 - When a location is disconnected, certain configurations are lost. Administrators must reconfigure aspects such as Associate PSTN Number Ranges prior to reconnecting the location.
-

Via the *Operations Tools* Menu

Procedure

To connect (activate) a location using the *Operations Tools* menu:

Step 1 Browse to *General Tools > Operations Tools > Activate Locations*.

Step 2 Click the **Activate** button adjacent to the relevant location.

Step 3 Enter the following parameters in the associated fields (note that these fields are available only if matching models are found):

- Pattern (#CLOCPATTERN#) - This is a free-format text entry that replaces the #CLOCPATTERN# variable in the models. This field is available only if route patterns and/or translation patterns are found for model name/s matching the *ConnectLocation* name.
Caution: If the pattern entered here already exists in the same partition selected from the *ConnectLocation* model name suffix, then the existing pattern will be overwritten on the Unified CM. This includes all calling/called transformation patterns, route patterns, translation patterns, hunt pilots and directory numbers.
- Model name suffix - Select from the drop-down list. This drop-down list contains the suffixes for all matching models. This field is available only if route patterns and/or translation patterns are found for model name/s matching the *ConnectLocation-* name. A *None* option is available in order to skip IPPBX provisioning. However make sure that there is no model name called *ConnectLocation-* (with a blank prefix), as CUCDM would then identify this as the model that you want to provision to the IPPBX.

Step 4 Click the **Activate** button to activate the selected location.

Note

- If a site is already connected, the **Activate** button is not available in the GUI as a connected location cannot be connected again.

- When a location is disconnected, certain configurations are lost. Administrators must reconfigure aspects such as Associate PSTN Number Ranges prior to reconnecting the location.

Associate PSTN Number Ranges and Connect Location

Associate PSTN Number Ranges are managed via the *Associate PSTN Number Range* sheet within the *09-LocAdmin* workbook. The sheet has a *Load Flag* column that enables administrators to specify how they would like the associations to be handled.

Note

The load flag can only be set via the bulk loaders.

The options for this column are Y or N:

- **Y:** If the flag is set to Y, the associateFNN logic and models are run. This is supported for all devices such as PGW-mmml, PGW-x10, IPPBX, GK and sets.
- **N:** If the load flag is set to N, the CUCDM completes the database provisioning of the transaction but does not communicate with any of the devices.

When connecting a location, the CUCDM deploys all associated numbers that have been associated using the N flag within the bulk loader sheets.

Note

- When loading FNNs via the loader and the location is already connected, no more FNNs can be loaded with the load flag set to N.
 - Disconnecting the location disassociates all numbers. In the case of FNNs with the load flag set to Y, the numbers remain within the location but are no longer be associated. Before connecting the location again, the numbers must be associated again using the bulk loader 09-LocAdmin workbook. However, when a location is disconnected all the FNNs with the load flag set to N are temporarily disassociated and automatically re-associated to the original FNN ranges when the location is connected again.
-

Additional References

For more information on AssociateFNN and Connect Location, refer to the following system guides:

- AssociateFNN Guide
- IOS Model Guide
- Call Manager Model Guide
- PGW Model Guide

Feature Display Policies

An end user is associated to a Feature Display Policy (FDP) when registered on the system. The FDP determines which system features are accessible to the end user via Self Care. The FDP also determines whether an accessible feature is 'read only' (not editable) or 'read write' (editable). The FDP can furthermore determine whether all individual fields (or settings) related to a feature are 'hidden', 'read only' or 'read write'.

In other words, a feature display policy determines an end user's access levels to system features and settings.

It is possible to assign policies to individual end users, or assign them as default policies to providers, resellers, buildings and customers.

Feature Display Policies are managed via *Setup Tools > Feature Display Policies*.

Procedure

Specifying a System Default Feature Display Policy

To specify a System Default Feature Display Policy:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
- Step 2** Select the *System Default* radio button adjacent to the relevant policy.
- Step 3** Click the **Update** button.

Bulk Loading Feature Display Policies

All values for setting up feature display policies and groups can be added using the bulk loaders. A sample loader sheet called *Feature Display Policies.xml* is available in the *1-Basedata.xml* workbook from the *Bulk Load Samples* page on the system GUI.

Adding a Feature Display Policy

Procedure

Adding a New Feature Display Policy

To add a feature display policy:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
- Step 2** Click the **Add** button.
- Step 3** Enter the *Policy Name* and *Description*.
- Step 4** For each Menu Item's Form Object, select from the *Apply to All (Access Type)* drop-down list the value that determines the end user's access level to the feature. The following values are available in the drop-down list: "Hidden", "Read Only", "Read Write", "Individual".

Selecting "Hidden", "Read Only" or "Read Write" applies the end user's access level to the entire *Form Object* and all its associated *Form Settings*. However, selecting the "Individual" option expands the Form Object section dynamically to display all the associated Form Settings for which individual *Access Type* settings can be selected from a drop-down list. The following values are available in the drop-down list: "Hidden", "Read Only" and "Read Write".

- Step 5** Click the **Add** button. The Feature Display Policy is added to the system.

Note

- The following *Form Objects* are governed at that level only and do not contain *Form Settings*:
 - Advanced Settings (part of the My Phones menu Item)

- Presence Monitor (part of the Presence menu item)
- Alternate Extensions (part of the Voicemail menu item)
- Caller Input (part of the Voicemail menu item)
- Voicemail Notifications (part of the Voicemail menu item)
- Voicemail Details (part of the Voicemail menu item)
- The system prevents non-editable fields from being set to "Read-Write".
- Setting certain mandatory fields to "Hidden" or "Read Only", may result in the failure of associated Self Care transactions.
- Not all settings for an entity have the "hidden" option available due to this data being critical to the identification of the entity to the user using the system. This ensures the user is clear on which entity they are viewing/affecting.
- The *Apply to All settings* for a form object does not overwrite a form setting if that form setting is more restrictive than the apply to all drop-down.

The following Form Objects are covered by FDP:

Table 2. Menu Items and Form Objects covered by FDPs

Field	Description
Menu Item: Details	
Account Details	Details of the end user, such as email address, extension directory, first name, last name and middler name.
Menu Item: Extension Mobility	
Apply Line Setting	Controls the visibility of the checkboxes and button used to 'Apply' the Private Line settings of the source device to devices sharing that line.
Extension Mobility Details	The details of a user's extension mobility profile, e.g. Description, Feature Group, Mobility Profile Name, Phone Locale and Privacy.
Line Details	The line details of the extension mobility, such as cloned, extension and shared.
Line Features	The line features of the extension mobility. These include, agent line, alerting name, call forward all, call forward all to voicemail, call forward busy, call forward busy internal, call forward no answer, call forward no answer external, call forward no coverage, call forward no answer ring duration, call forward not registered, call forward on CTI failure, MOH, and PLAR.
Multiple Call/Call Waiting Settings	The multiple call/call waiting Settings of the extension mobility, such as busy trigger and max calls waiting.
Phone Line Features	The phone line features of the extension mobility. These include, caller name, dialled number, display name, label ASCII, redirected number and ring setting phone idle.
Menu Item: Mobile Identity	
Remote Destinations	The details of a Mobile Identity's remote destinations, such as answer too late, answer too soon, country code, enable mobile connection, FMC, FMC primary, mobile phone, remote name and remote number.

Field	Description
Menu Item: My Phones	
Advanced Settings	The advanced settings associated with the end user's phone.
Apply Line Settings	Controls the visibility of the checkboxes and button used to 'Apply' the Private Line settings of the source device to devices sharing that line.
Line Details	The details of the line, such as cloned, extension and shared.
Line Features	Line features, including agent line, alerting name, auto answer, call forward settings, line class of service, music on hold and PLAR.
Multiple Call/Call Waiting Settings	Details of the phone's multiple call/call waiting settings, such as busy trigger and max calls waiting.
Phone Details	Details of the phone details, such as date registered, feature group, phone type and unique device name.
Phone Features	All the features available on the phone, such as built in bridge status, cache username, extension mobility, privacy, service URLs and SRST.
Phone Line Features	Features available on the phone line, including caller name, caller number, display name, label, message waiting lamp policy, redirected number and ring setting phone idle..
Phone Settings	The phone settings, including default music on hold and locale.
Menu Item: Presence	
Presence Config	Settings to enable CUPC, enable IM and Presence, and enable Presence for the end user.
Presence Monitor	Setting to monitor Presence.
Menu Item: Single Number Reach	
Remote Destinations	The details the remote destinations for SNR, such as answer too late, answer too soon, country code, FMC, mobile phone, remote name, remote number and ring schedule.
SNR Settings	The SNR settings, including primary device, privacy and the profile description.
Menu Item: Voicemail	
Alternate Extensions	The alternate extensions for the voicemail account.
Caller Input	The voicemail caller input details.
Voicemail Details	General voicemail details.
Voicemail Notifications	Voicemail notification details.

Adding Feature Display Policy Groups

Procedure

Adding new Feature Groups

To add a new Feature Display Policy Group:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
- Step 2** Click the **Add Group** button.

- Step 3** Enter a group name, an alternative title for the group, specify group visibility (affects all feature fields in the group) and display order for the group.

For each group, select the feature fields that belong to the group. For each selected field, specify:

- *Access type*: Read-write, read or hidden
- *Display order within the group*: Since certain fields are related, the system lists feature fields on this screen in an order that makes logical sense and it is advisable that field display order settings mimic this.
- *Default value*: This value will be used to pre-populate the field when displayed to the user.

- Step 4** Click the **Add** button when complete.
-

The group will be added to the system.

Bulk Loading Feature Display Policies and Groups

All values for setting up feature display policies and groups can be entered using the Bulk Loader facility. A sample loader is available from the main menu at *Setup Tools > Bulk Load Samples*

Feature Display Policy Management

Procedure

Modifying and Deleting Feature Display Policies

To modify or delete a feature display policy:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
- Step 2** Select the required Policy *Name* (active text link).
- Step 3** To modify the policy, modify the required fields (see above table), and then click the **Modify** button.

OR

Note

- It is not possible to delete the system default policy.
- When a Feature Display Policy which is in use by an end user is deleted, the end user's feature display policy reverts to the default FDP. In the case where an FDP has been assigned to a customer this default uses the assigned FDP; if no FDP has been assigned to anywhere in that user's hierarchy then it reverts back to the system's default.

- Step 4** To delete the policy, click the **Delete** button.
-

The Feature Display Policy is updated within the system.

Assigning Feature Display Policies

Once a policy is defined, it can be assigned to individual users, or in bulk to a provider, reseller, building or customer level.

Procedure

Assigning Feature Display Policies to Multiple Users

Often policies are assigned to all users on a particular provider, reseller, building or customer:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
 - Step 2** Click the **Assign** button adjacent to the relevant policy.
 - Step 3** Select one or more options from the list then click the **Update** button.
-

Note

Use the *Ctrl* and *Shift* keys to make multiple selections.

Procedure

Assigning a Feature Display Policy to a Single User

Note

It is important to note that only end users may be assigned a Feature Display Policy. In order for users to be associated to the assigned FDP, their FDPs must be set to 'Default' when they are registered as users on the system. Users who have been associated to specific FDPs other than 'Default' are not associated to the assigned FDP.

To assign a policy to a single user:

- Step 1** Browse to *Location Administration > End Users*.
 - Step 2** On the User Details screen, select the relevant Feature Display Policy from the drop-down list then click the **Modify** button.
-

Note

Policies assigned directly to users this way override policies assigned to users on provider, reseller or customer level. Therefore, for any user to inherit a policy set at a provider, reseller or customer level, the user's Feature Display Policy must be set to *<Default>*.

Shared SLC

This functionality allows a single site-code to be shared within a group of locations called Linked Locations. This would allow extension only dialing and use of a single site-code to call any phones within the linked locations. It also allows hunt groups to include lines from any location within the linked locations.

In any linked location group, one of the locations is a linked location parent which provides the site-code for the group. All other locations which share the site-code with linked location parent are called linked location child. Linked Locations can exist within different divisions but they should be in a single customer.

The list of details inherited by the child from the parent includes:

- Site Code

- Extension Length
- Hardware Group
- PBX Template
- Global site partition of the parent used for all children (used for all the fints in the locations)

All other settings/resources for a child location are independent of the parent (e.g. published number, emergency number, voicemail, gateways, etc).

Note

While not inherited from the parent, parent and child locations share Call Park ranges. It does not matter if the ranges are created at the parent or the child location, all locations that are part of the linked location setup will use the extension pool. Hence, parked call retrieval is possible across linked locations.

The following is a list of considerations for a linked location setup:

- Extension management is individual for each location and is not visible across locations. An extension added to a location needs to be unique and can't be used in any of the other linked locations as they all share a site code. This is enforced by the system.
- Linked locations have to be on the same IPPBX
- Linked Locations have to be in the same country
- All the resources in a location which use an extension
- Number Groups/Hunt Groups can span all the locations in the linked setup. All other location level entities which use extensions are limited to extensions in their location (e.g. Pickup Groups, etc).
- Linked locations can cross Divisions, but must be within the same customer.
- There is no limit to the number of linked location child. The limit is really driven by the extension requirements in the locations.
- Add Location for the parent location calls the RegisterPhone Cisco Unified Communications Manager model, while AddLocation for the child locations calls the RegisterPhoneLinkedLocation model.
- For the ConnectLocation transaction, the parent location uses ConnectLocation, while the child uses the model name ConnectLocationLinkedLocation.

Adding a Linked Location Parent

To add a Linked Location Parent browse to *General Administration > Locations* and click the **Add** button. Select *Linked Location Parent* from the *Is Linked Location* drop-down list and configure the rest of the settings for the location as usual and click the **Add** button.

The CCM model used for this is *RegisterPhone* as per a standard location. The PGW mmlscriptname is AddLocation as per a standard location.

Converting a Standard Location to Linked Location Parent

To convert a standard location to Linked Location Parent, browse to *General Administration > Locations* and select the *Location* . Check the *Linked Location Parent* checkbox and click the **Modify** button.

Converting a to Linked Location Parent a Standard Location

Linked Location Parent can be converted to a Standard Location if it does not have any other linked location child associated to it. To convert a Linked Location Parent to a Standard Location, browse to *General Administration > Locations* and select the *Location* . Uncheck the *Linked Location Parent* checkbox and click the **Modify** button.

Adding a Linked Location Child

To add a Linked Location Child, browse to *General Administration > Locations* and click the **Add** button. Select *Linked Location Child* from the *Is Linked Location* drop-down list. Select the Linked Location Parent for the location by selecting a location in the *Linked Location Parent* drop-down list and clicking the **Next** button.

Note

The parent drop-down will be populated with *None* if no linked location parents are currently in that customer.

The Hardware Group, PBX Template, site-code and Extension Length settings for Linked Location Child are derived from Linked Location Parent. Unique extension ranges are selected for each location in the linked locations as extensions cannot be shared between them. The CCM model used for this is *RegisterPhoneLinkedLocation* . The PGW mmlscriptname is *AddLocation*, as per a standard location.

Reassigning the Linked Location Parent Role in Linked Locations

To reassign the Linked Location Parent Role in Linked Location Group navigate to browse to *General Administration > Locations* . A hyperlink will be available for Linked Location Parent and Linked Location Child under the column *Location Type* will lead to the *Linked Locations Management* screen. A link to the *Linked Location Management* screen will also be available on the *Manage Locations* page for *Linked Location Parent* and *Linked Location child* besides the Site-code setting.

This page would list all the Linked Locations for the site-code with a configurable radio button which would be set for the existing Linked Location Parent. Select the radio button for the *Linked Location child* that will be reassigned as Linked Location Parent and click the **Modify** button.

This transaction initiates a transaction which:

- Calls the Driver_IPPBX to change the site partition name for the parent to use the new parent's id. It also calls the CCM model with the model name *RegisterPhoneModLinkedLocationParent* to add any partitions/CSS/Route Patterns/Translation Patterns to the location as required.
- Calls the Driver_Transit with the mmlscriptname *AddLocationModLinkedLocation*.

Note

If the *RegisterPhone* and *RegisterPhoneLinkedLocation* models do not match exactly, deleting the old parent can be problematic as some partitions and route patterns etc. might still be associated to the parent.

Hunt Group/Number Groups for Linked Location

The lines associated in various linked location would be available for addition in number groups within linked locations. To add a line to a number group in a different linked location, browse to

Location Administration > Number Groups and select the *linked location* in which the number group needs to be added, and then click the **Add** button. The lines from different linked location would be marked with the location name and would be available to be added as a line number in the number group.

Location Level Operations Tool to Delete Lines of Different Linked Location from the Number Group

A Location Level operations tool is available in *General Tools > Operations Tools*, called *Delete all lines from number groups of linked locations*. This will disassociate all the lines of different linked location from the number group of the location.

Bulk Loading Linked Locations

Location's bulk loader consists of a new optional column called as *Linked Location*. This column takes in the values *None* for Standard Location, *Linked Location Parent* and *Linked Location Child*.

For Linked Location Child the Hardware Group, PBX Template and Extension Length settings are optional as they are derived from linked location parent and can be left blank. Also, the parent is worked out based on the SLC provided for the location so a parent location setting is not required.

CTI/TAPI Management

The section details how CTI Route Points and Ports added at location level can be managed by the system.

Management of CTI Route Points and Ports

To manage CTI Route Points and Ports navigate to *Location Administration > Telephony*, select the location for which CTI Route Points and Ports needs to be managed and then select the *CTI Management* link. This leads to a screen that presents two options *CTI Route Points* and *CTI Ports*.

To manage CTI Route Points, select *CTI Route Points*, to manage Ports, select *CTI Ports*.

There is a global setting which allows the override of the default partition selection for the DNs assigned to CTI Route Points and Ports.

Altering the Partition used for CTI Route Points and CTI Ports

There is a global setting in the CCM model which can be used to override the partition used for the CTI RP or Port DNs. These are in the CCM model on the sheet *CCM 7.1.0 - Global Settings* with the column names of *CTI RP Partition* and *CTI Port Partition*.

You can include any partition name that is loaded elsewhere in the model. This is used to override the normal partition selection for DNs which is based on the *Site Partition Name* column in that global settings sheet.

Adding CTI Route Points/ CTI Ports

Setting a Feature Group for use with CTI Route Points/ Ports

To add a feature group, navigate to *General Administration > Feature Group* and click the **Add** button. A feature group consisting of the following features needs to be added for CTI Route Points/Ports:

- Outbound Call Limitations
- Call Forward Limitations
- Secondary Call Forward Limitations
- Voicemail Template
- Call forward - always
- Call forward when busy
- Call forward if no answer
- Call forward on non registered
- Call forward all calls to voicemail.
- Call forward on busy to voicemail
- Call forward on no answer to voicemail
- Call forward on non registered to voicemail
- Call forward on no coverage
- Call Forward on No Coverage to Voicemail
- Call forward on CTI failure
- Call Forward On CTI Failure to Voicemail
- Call forward calling search space activation policy
- Hold reversion ring duration
- Hold reversion notification interval
- Label
- Label ASCII
- Display name (Caller Line ID)
- Display name ASCII
- Line mask
- No answer ring duration
- Alerting Name
- Alerting name ASCII
- Forwarded Call Display - Caller Name
- Forwarded Call Display - Caller Number
- Forwarded Call Display - Redirected Number
- Forwarded Call Display - Dialed Number

Procedure

Adding a CTI Route Point

To add CTI Route Points:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select the *CTI Management* link.
- Step 3** Select the *CTI Route Points* link.
- Step 4** Click the **Add** button.
- Step 5** Under *Details*, the following fields need to be configured to add a CTI Route Point/Port:
 - Device Name. This is a mandatory field.
 - Description
 - Device Pool: Select from the list of available Device Pools. This list displays all device pools that are not of type System or SRST
 - User Locale: Select from the list of country codes
 - Number: Select from the list of extension numbers available in the location
 - Feature Group: Select from the list of feature group which would define the features for the number selected.

Click the **Next** button.

Procedure

Adding a CTI Port

To add CTI Ports:

- Step 1** Browse to *Location Administration > Telephony*.
 - Step 2** Select the *CTI Management* link.
 - Step 3** Select the *CTI Ports* link.
 - Step 4** Click the **Add** button.
 - Step 5** Under *Details*, the following fields need to be configured to add a CTI Route Point/Port:
 - Device Name. This is a mandatory field.
 - Description
 - Device Pool: Select from the list of available Device Pools. This list displays all device pools that are not of type System or SRST
 - User Locale: Select from the list of country codes
 - Number: Select from the list of extension numbers available in the location
 - Feature Group: Select from the list of feature group which would define the features for the number selected.
- Then click the **Next** button.
- Step 6** Provide the settings for the features available in the feature group and click the **Add** button. The CTI Ports is added to the system.

Note

- This also adds the CTI Route Point /Port to the IPPBX supported by the location.
- The call forwarding options set in the system are automatically provisioned as call forwarding options in Cisco Unified Communications Manager (Unified CM). However, if the checkbox for any call forward to Voice Mail scenario is enabled, but a destination number for the corresponding scenario is also provided, then both are provisioned on Unified CM, but the call forward to Voice Mail setting overrides the destination number.
- The Voice Mail profile name is configured on Unified CM.

Line Setting Information

Procedure

Step 1 Complete all of the required line setting fields (see table below).

Field	Description	Updated?	Remarks
Label	The line label if configured (different than default).	Read Only	
Label ASCII	The line's ASCII label if configured (different than default).	Read Only	
Display name (Caller Line ID)	The identifier information that is sent with an outbound call made from this line.	Yes	<p>The phone of the call receiver displays this information as part of the identification of the caller.</p> <p>Best Practice:</p> <ul style="list-style-type: none"> • Based on organization standards it is recommended to have a meaningful value in this field. • Take into account the various phone type (with different screens size) when considering the standards for this field.
Display name ASCII	The identifier information that is sent with an outbound call made from this line.	Yes	<p>The phone of the call receiver displays this information as part of the identification of the caller.</p> <p>Best Practice:</p> <ul style="list-style-type: none"> • Based on organization standards it is recommended to have a meaningful value in this field. • Take into account the various phone type (with different screens size) when considering the standards for this field.

Field	Description	Updated?	Remarks
Line mask	Line Mask is the DDI information at the top of the phone.	Yes	<p>Default:</p> <ul style="list-style-type: none">• If the phone has a DDI, it is presented in the mask field.• If the phone does not have a DDI and the location has a PSTN Published Number, the PSTN published number is presented.• If the phone does not have a DDI and the location does not have a PSTN Published Number, the local extension is presented.• In case the phone was registered with an internal extension only and associated later with a DDI, the E164 Mask does not change until the phone is unregistered and re-registered. Alternatively, you can run the Ops tool <i>Update All Phone/Extension Mobility/CTI Line Masks At Location</i> after the associate/dissociate task to update the relevant line mask/s at the location - see Operations Tools on page 950 if required.

Field	Description	Updated?	Remarks
Message waiting lamp policy	Use this option to set the Message Waiting Lamp behavior	<p>Yes</p> <ul style="list-style-type: none"> • "Use System Policy" follows the policy determined by your system administrator. Contact your phone system administrator if you are not sure what policy is used. • "Light and Prompt" causes the lamp to light and displays the prompt if there is a message waiting on this line of your phone. • "Prompt only" displays the prompt if a message is waiting on the primary line • "Light only" lights the message-waiting lamp if a message is waiting on the primary line. • "None" causes the lamp to stay off even when you have messages waiting on this line. The message waiting indicator on your phone's display still shows if you have messages on this line. 	<p>This policy ONLY affects the right light on the phone's handset. The message waiting indicator on the phone's display is always active for all lines.</p> <p>The message-waiting policy that you choose depends on the needs of your users. For example, an administrative assistant, who shares the manager's directory number as a secondary directory number, may want to have the policy set to Light and Prompt. The administrator can see whether the manager's line has pending voice messages. General office members, who share a line appearance with a co-worker, might set the policy, so the indicator lights only when messages are pending for the primary line appearance.</p>
Ring setting - Phone idle	Defines the way the line on your phone rings when you receive a call while phone is not in use (idle).	<p>Yes - From list</p> <ul style="list-style-type: none"> • Use System Default • Disable • Flash only • Ring once • Ring • Beep only 	<p>You can set phone to ring differently when a new call arrives while your phone is not being used (idle).</p> <p>Select from the drop-down selection list. The default value is defined when the system is set-up.</p>
Ring Setting - Phone active	Defines the way the line on your phone rings when you receive a call while you are on the phone already.	<p>Yes - From list</p> <ul style="list-style-type: none"> • Use System Default • Disable • Flash only • Ring once • Ring • Beep only 	<p>You can set phone to ring differently when a new call arrives while you are on the phone (in use).</p> <p>Select from the drop-down list. The default value is defined when the system is setup.</p>

Field	Description	Updated?	Remarks
Max calls waiting	The maximum number of calls that can be queued for waiting. Once this number is reached, the next caller gets a busy tone.	Yes	Select from the drop-down list. The default value and the allowed values on the selection list are configured using the phone type templates by the division or customer administrator.
Forwarded Call Display - Caller Name	This line feature allows a receiver of forwarded calls to display the name of the call originator. When a line is first registered, this has a default value of 'True'.	Select the checkbox to turn feature on.	
Forwarded Call Display - Caller Number	This line feature allows a receiver of forwarded calls to display the number of the call originator. When a line is first registered, this has a default value of 'False'.	Select the checkbox to turn feature on.	
Forwarded Call Display - Dialed Number	This line feature allows a receiver of forwarded calls to display the line number that the originator attempted to reach. When a line is first registered, this has a default value of 'True'.	Select the checkbox to turn feature on.	
Forwarded Call Display - Redirected Number	This line feature allows a receiver of forwarded calls to display the number that was redirected. When a line is first registered, this has a default value of 'False'.	Select the checkbox to turn feature on.	
Call waiting busy trigger	This field is used to specify the maximum number of calls to be presented at the line. For example, if the maximum number of calls is set at 50 and the busy trigger is set to 40, incoming call 41 is rejected with a busy cause (and is forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls are rejected.	Yes	Select from the drop-down selection list. The default value and the allowed values on the selection list are configured using the phone type templates by the division or customer administrator.
Alerting Name	The device's alerting name.	Yes	
Alerting Name ASCII	The device's alerting name ASCII value.	Yes	

Field	Description	Updated?	Remarks
Auto answer	Allows you to connect incoming calls automatically after a ring or two (without pressing a button or picking up the handset).	<p>Yes from the following list:</p> <ul style="list-style-type: none"> "Auto Answer Off" Auto Answer is disabled. "Auto Answer with Headset" You can configure lines on specific phones to automatically connect to incoming calls when the headset key is activated. The phone cannot be busy with an active call and the headset key must be engaged to automatically answer calls. Incoming calls are automatically answered one by one on the phone as long as the headset light remains lit. You can specify one or more lines for headset auto-answer. "Auto Answer with Speaker phone" when an incoming call is received, the speaker phone of your device is automatically turned ON when you receive the call. 	<p>Auto Answer can be useful if you receive a high volume of calls.</p> <p>Your system administrator enables Auto Answer to work with either your speaker phone or headset.</p>
Call forward - always	A number to which calls should be forwarded under all circumstances.	Yes	<p>Number typed in needs to be exactly as dialed.</p> <p>Note: This value is synced in a similar manner to the <i>Call forward all calls to voicemail</i> setting (see below).</p> <p>This setting takes precedence over all other call forward settings, except <i>Call forward all calls to voicemail</i> (see below).</p>
Call forward when busy	A telephone number to which calls should be forwarded when the phone is busy.	Yes	Number typed in needs to be exactly as dialed.
Call forward if no answer	A telephone number to which calls should be forwarded if the phone rings but is not answered.	Yes	Number typed in needs to be exactly as dialed.
Call forward on non registered	A telephone number to which calls should be forwarded if the phone is not able to register.	Yes	Number typed in needs to be exactly as dialed.
Call forward on no bandwidth	A telephone number to which calls should be forwarded if network bandwidth is insufficient to complete the call.	Yes	Number typed in needs to be exactly as dialed.

Field	Description	Updated?	Remarks
Call forward all calls to voicemail	Forwarded all calls to the Voice-mail box associated with this line.	<p>Disable the checkbox (default) - the feature is off</p> <p>Enable the checkbox to turn feature on</p>	<p>Note: If there is no connectivity between the CUCDM and Cisco Unified Communications Manager (Unified CM), then an error message is displayed next to the <i>Call forward all calls to voice-mail</i> field, informing you that these values may be out of sync. In this case, an additional button Sync with Call Manager is provided next to the Modify button at the bottom of the page. Click the Sync with Call Manager button to manually sync these values with Unified CM when connectivity has been restored.</p> <p>This setting takes precedence over all other call forward settings. See also <i>Call forward - always</i> setting above.</p>
Call Forward calls on busy to voice-mail	Send calls to voicemail when the phone is busy.	<p>Disable the checkbox (default) - the feature is off.</p> <p>Enable the checkbox to turn feature on.</p>	
Call forward on no answer to voicemail	Send calls to voicemail when the phone rings but is not answered.	<p>Disable the checkbox (default) - the feature is off.</p> <p>Enable the checkbox to turn feature on.</p>	
Call forward on non registered to voicemail	Send calls to voicemail when the phone is not able to register.	<p>Disable the checkbox (default) - the feature is off.</p> <p>Enable the checkbox to turn feature on.</p>	
Call forward on no bandwidth to voice-mail	Send calls to voicemail when network bandwidth is insufficient to complete the call.	<p>Disable the checkbox (default) - the feature is off.</p> <p>Enable the checkbox to turn feature on.</p>	

Step 2 Click the **Add** button when complete. The CTI route point is added to the system.

Note

The call forwarding options set in the system are automatically provisioned as call forwarding options in Cisco Unified Communications Manager (Unified CM). However, if the checkbox for any call forward to Voice Mail scenario is enabled, but a destination number (or URI) for the corresponding scenario is also provided, then both are provisioned on Unified CM, but the call forward to Voice Mail setting overrides the destination number (or URI).

Modifying CTI Route Points/ Ports

Procedure

To Modify CTI Route Points:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select the CTI Management link.
- Step 3** Select the CTI Route Points link.
- Step 4** Select the device name to be modified.
- Step 5** Make the required changes and click the **Modify** button. The CTI Route points are modified.

Procedure

To Modify CTI Ports:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select the *CTI Management* link.
- Step 3** Select the *CTI Ports* link.
- Step 4** Select the device name to be modified. Under details the following settings can be modified:
 - Description
 - User Locale
 - Feature Settings: Modify the settings for the features available in the feature group.

Note

If there is no connectivity between the system and Cisco Unified Communications Manager (Unified CM), then an error message is displayed next to the *Call forward all calls to voicemail* field, informing you that these values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the page. Click the **Sync with Call Manager** button to manually sync these values with Unified CM when connectivity has been restored. The *Call forward - always* field is synced in a similar manner to the *Call forward all calls to voicemail* field.

- Step 5** Click the **Modify** button. The CTI Ports are modified.

Note

- This also modifies the CTI Route Point /Port on the IPPBX supported by the location.
- The Voice Mail profile name is configured on Unified CM.

Deleting a CTI Route Point/Port

Procedure

To delete CTI Route Points:

- Step 1** Browse to *Location Administration > Telephony*.
 - Step 2** Select the *CTI Management* link.
 - Step 3** Select the *CTI Route Points* link.
 - Step 4** Select the device name to be deleted.
 - Step 5** Click the **Delete** button. The CTI Route Points are deleted.
-

Deleting CTI Ports

Procedure

To delete CTI Ports:

- Step 1** Browse to *Location Administration > Telephony*.
 - Step 2** Select the *CTI Management* link.
 - Step 3** Select the *CTI Ports* link.
 - Step 4** Select the device name to be deleted.
 - Step 5** Click the **Delete** button. The CTI Port is deleted.
-

Note

This also deletes the CTI Route Point/Port from the IPPBX supported by the location.

Transit Deferral

The Transit Deferral feature is intended to reduce the time taken by large numbers of Transit Switch transactions initiated by the bulk loaders. At the end of each PGW provisioning update, the PGW deploys or copies the new configuration; this action can take several seconds to complete. By combining several PGW updates into a single batch the final deployment overhead is shared by several transactions thus reducing the overall processing time.

When the feature is enabled the transactions appears to function as normal, but instead of sending individual provisioning requests to the PGW, the system accumulates this information. The transactions will appear to complete successfully. After a certain number of configuration steps have completed, the system will insert a Transit Defer transaction. This transaction passes each of the PGW configuration steps accumulated so far and uses them to provision the PGW, with a single deploy/copy operation for the entire batch.

Enabling Deferral

The Transit Deferral feature is enabled by assigning a value greater than zero to the *TransitDefer* global setting (*Setup Tools > Global Settings > TransitDefer*). This value specifies the number of provisioning steps (rows in the bulk loader worksheet) to be executed as a single deferred step.

Error Handling

If any failures occur during the deferred processing, then all of the transactions in the deferred group will be rolled back and marked as failed. An appropriate error message will be assigned to the transactions that were rolled back.

Note that the system-generated Transit Defer transaction will only be marked as having failed if it encountered an unexpected error. It will be considered to have succeeded even if some or all of the deferred provisioning steps failed.

Affected Transactions

At present the Transit Defer feature is only applicable to the *Add Locations* and *Associate PSTN Number Range* bulk load work sheets.

Session Border Controllers

This section covers the adding and management of Session Border Controllers (SBC).

Session Border Controller Management (SBC)

The Session Border Controller (SBC) functionality in the system provides the ability to create the SBC and connect it to a Transit Switch (Cisco PGW). The system does not configure the SBC device, however it does configure the connections and related dial plan into the Transit device as defined in the models.

The main functionality for the Session Border Controllers in the system today is for connectivity of unmanaged locations. Once setup and connected to a transit, they can be associated with a location to provide the connectivity for that legacy site to the Cisco HCS architecture. In the future additional capabilities could be added for PSTN connectivity as an example.

This section covers the setup and management of the SBC and connecting it to an unmanaged location. For more details on the setup/management of unmanaged locations, please see the unmanaged locations section.

The Session Border Controller management functionality is accessed by browsing to *Network > Session Border Controllers*.

The following search criteria are available for SBCs:

- Name
- IP Address

The following columns are available on the Search Results page:

- Name of SBC
- Description
- Domain Name
- First IP Address added

The following functionality is available from the Session Border Controller page:

- Add SBC button: Leads to the Add SBC page
- SBC link: Selecting the name (active text link) of the SBC will open the Manage SBC page
- SBC Connectivity button: Will launch the SBC Connectivity page for that SBC to add a connection

SBCs are added to the system by clicking the **Add** button on the main SBC page.

The following details need to be provided in the SBC Details section of the Add form:

- **Name of the SBC:** This is a mandatory field and must be unique
- **Description :** An optional short description of the SBC being added
- **Domain Name:** This is a mandatory field

The following details need to be provided in the SBC Interface Details section of the Add form:

- **IP Address blocks:** A block for each octet
- **Range:** Specify range for last octet

The following buttons are available on the SBC Interface Details section of the Add form:

- **Add to List** button: Adds the specified IP Address to the list box
- **Delete from List** button: Deletes the selected IP Address

There are two available methods to complete the add process:

- Clicking the **Add** button: This will add the SBC and relevant Interfaces to the system.
- Clicking the **Add & Connect** button: This will launch the **Add Connectivity** page with the supplied SBC information.

Add an SBC

Procedure

Adding an SBC

Follow these step to add an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the **Add** button
- Step 3** Complete the required fields.

The following fields are available:

Field	Description
<i>Name of the SBC</i>	The name of the SBC being added. This is a mandatory field and must be unique
<i>Description</i>	An optional short description of the SBC being added
<i>Domain Name</i>	The domain to which the SBC is being added. This is a mandatory field.
<i>IP Address blocks</i>	Enter each octet of the IP address in the relevant field. To add an IP address, enter the IP address in the field and select the Add to List button. To delete an IP address from the list, select the IP address and then select the Delete from List button.
<i>Range</i>	Define the range of IP addresses by specifying the last octet of the range. The use of this field is optional. To add an IP address range, enter the last octet of the range you would like to add, then select the Add to List button. For example, to add all IP address from 1.1.1.1 to 1.1.1.100, enter the IP address 1.1.1.1 and enter the Range as 100. All IP addresses from 1.1.1.1 to 1.1.1.100 will be added to the list.

- Step 4** There are two available methods to complete the add process:
- a** Select the **Add** button.

The SBC and all of the relevant Interfaces will be added to the system.

Or

- b** Select the **Add & Connect** button

The *Add Connectivity* page will launch with the supplied SBC information.

Manage Session Border Controller

Also refer to :

- [Session Border Controller Management \(SBC\) on page 453](#)
- [SBC Connectivity on page 461](#)
- [Manage SBC Interfaces on page 459](#)
- [SBC Connected Locations on page 458](#)

When viewing the details of an SBC, the following details are available:

- **Id:** The Id of the SBC in the system, this is a read only field.
- **Name:** The name of the SBC. This field can be modified and is mandatory.
- **Description:** Description of the SBC. This field can be modified.
- **Domain Name:** A mandatory field, this field is modifiable only if the SBC is not currently connected.

The following buttons are available on this page:

- Connectivity button: Flows to the SBC Connectivity page - see: [SBC Connectivity on page 461](#)
- Interfaces button: Flows to the SBC Interfaces page
- View Locations button: Flows to the SBC Locations page
- Delete button: Deletes the selected SBC
- Modify button: Saves the modification made to the SBC

Procedure

Managing an SBC

Follow these steps to manage an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the **name** of the SBC (active text link) that you would like to manage
- Step 3** Modify the required fields and select the **Modify** button

The SBC will be updated within the system.

The following functionality is available from the Manage SBC page:

- **Connectivity** button: Opens the SBC Connectivity page

- **Interfaces** button: Opens the SBC Interfaces page
 - **View Locations** button: Open the SBC Locations page
-

Manage Connection

The SBC Device Details section of the page displays the following information:

- **Device Type:** This field is read only and should read SBC
- **Device Name:** This field is read only and is the name of the SBC

The SBC Connected Device section of the page displays the following information:

- **Device Type:** This field is read only and should read Transit Switch
- **Device Name:** This field is read only and is the name of the Transit Switch
- **Trunk Code:** This field is read only and is the Trunk code allocated to the connection

Clicking the **Delete** button will delete the connection.

The SBC Connected Interface section of the page displays the following information:

- **IP Address:** IP address of the connected SBC interface
- **Port:** The Port assigned to the interface
- **Priority:** The priority assigned to the interface
- **Trunk Code:** The Trunk code allocated to the interface
- **Transit Interface:** The Transit interface being used in the connection

Clicking the **Disconnect** button will disconnect the selected interfaces.

The *SBC Available Interfaces* section of the page displays the following information:

- **IP Address:** The unconnected interface available for connection
- **Port:** Assign the port to be used in the connection
- **Priority:** Assign the priority associated with the interface

Clicking the **Connect** button will connect the selected interfaces.

Procedure

Manage Connection

Follow these steps to manage a connection for an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
 - Step 2** Select the **name** of the SBC (active text link) that you would like to manage
 - Step 3** Select the **Connectivity** button
 - Step 4** Select the **Manage** button adjacent to the connection that you would like to manage
-

The following information will be displayed:

Field	Description
Device Details	
<i>Device Type</i>	This field is read only and should read SBC
<i>Device Name</i>	This field is read only and is the name of the SBC
Connect Device Details	
<i>Device Type</i>	This field is read only and should read Transit Switch
<i>Device Name</i>	This field is read only and is the name of the Transit Switch
<i>Trunk Code</i>	This field is read only and is the Trunk code allocated to the connection
Connected Interfaces	
<i>IP Address</i>	IP address of the connected SBC interface
<i>Port</i>	The Port assigned to the interface
<i>Priority</i>	The priority assigned to the interface
<i>Trunk Code</i>	The Trunk code allocated to the interface
<i>Transit Interface</i>	The Transit interface being used in the connection
Available Interfaces	
<i>IP Address</i>	The unconnected interface available for connection
<i>Port</i>	Assign the port to be used in the connection
<i>Priority</i>	Assign the priority associated with the interface

Procedure

Connecting and Disconnecting interfaces

Follow these steps to Connect or Disconnect an interface from an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the name of the SBC (active text link) that you would like to modify
- Step 3** Select the **Connectivity** button
- Step 4** Select the **Manage** button adjacent to the connection that you would like to manage
- Step 5** To connect an interface, select the interface you would like to connect from the Available Interfaces section of the screen and select the **Connect** button.
- Or**
- Step 6** To disconnect an interface, select the interface you would like to disconnect from the Connected Interfaces section of the screen and select the **Disconnect** button.

The connection will be connected/disconnected.

Note

To connect and disconnect multiple interfaces at once, use the **Select All** and **Deselect All** buttons to control multiple selections within the relevant interface sections.

Deleting a Connection

Procedure

Deleting a Connection

Follow these steps to delete a connection from an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
 - Step 2** Select the **name** of the SBC (active text link) that you would like to modify
 - Step 3** Select the **Connectivity** button
 - Step 4** Select the **Manage** button adjacent to the connection that you would like to manage
 - Step 5** Select the **Delete** button
-

The connection will be deleted.

Procedure

Deleting an Interface

Follow these steps to delete an Interface:

- Step 1** Browse to *Network > Session Border Controllers*
 - Step 2** Select the **name** of the SBC (active text link) that you would like to modify.
 - Step 3** Select the **Interface** button then browse to the *Interface Details* section of the page
 - Step 4** Select the interfaces that you would like to delete then select the **Delete** button
-

The selected interface(s) will be deleted.

Note

- An interface may only be deleted if no device is currently connected to it.
 - Multiple interfaces may be deleted at once by selecting multiple interfaces.
-

SBC Connected Locations

The SBC Connected locations page is accessed by clicking the **View Locations** button. You are able to search using the following criteria:

- Location
- Connected Device

The results will include the following information:

- Reseller
- Customer

- Division
- Location
- Connected Device (The name of the Transit Switch)

Selecting the *Connection Details* link will launch the *Manage Connections* page.

Procedure

Viewing Locations

Follow these steps to view SBC connected locations:

Step 1 Select the relevant **SBC** name (active text link)

Step 2 Select the **View Locations** button

A list of locations will be displayed. The following columns are available on this page:

- Reseller
- Customer
- Division
- Location
- Connected Device (The name of the Transit Switch)

Note

Selecting the *Connection Details* link will launch the *Manage Connections* page.

Manage SBC Interfaces

The *Manage SBC Interfaces* page is accessed by clicking the **Interface** button.

The *Device Details* section of the page displays the following information:

- **Id** : This field is read only
- **Name**: This field is read only
- **Description**: This field is read only
- **Domain Name**: This field is read only

The *Interface Management* section of the page displays the following information:

- **IP Address blocks**: A block for each octet
- **Range**: Specify the range for last octet

The following buttons are available from the *Interface Management* section of the page:

- **Add to List** button: Adds IP Address to the list box
- **Delete from List** button: Deletes selected IP Address
- **Add** button: Used to add additional interfaces

The *Interface Details* section of the page displays the following information:

- **IP Address:** Interfaces of the SBC
- **Device Name:** Displays the name of the device connected to interface

Clicking the **Delete** button will delete the selected interfaces.

Note

An interface may only be deleted if no device is currently connected to it.

Procedure

View Interfaces

Follow these steps to manage the interfaces of an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the name of the SBC (active text link) that you would like to modify
- Step 3** Select the **Interface** button

The following information will be displayed:

Field	Description
Device Details	
<i>Id</i>	This field is read only on this screen. This is the ID of the selected SBC.
<i>Name</i>	This field is read only on this screen. This is the name of the selected SBC.
<i>Description</i>	This field is read only on this screen. This is an optional description for the selected SBC.
<i>Domain Name</i>	This field is read only on this screen. This is the domain name of the selected SBC.
Interface Management	
<i>IP Address blocks</i>	A block for each octet of the interfaces IP address
<i>Range</i>	Specify the range for last octet of the IP address range
Interface Details	
<i>IP Address</i>	The IP addresses of the interfaces of the SBC
<i>Device Name</i>	Displays the names of the devices connected to interface

Procedure

Managing the Interface List

The Interface List is managed from the *Interface Management* section of the *Manage SBC Interfaces* page.

Follow these steps to manage the interface list of an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the **name** of the SBC (active text link) that you would like to modify

- Step 3** Select the **Interface** button then browse to the *Interface Management* section of the page
- Step 4** To add a single IP address enter the required IP address then select the **Add to List** button.
- Or**
- To add a range of IP addresses, enter the required IP address and in the *Range* field, enter the last octet of the IP address range, then select the **Add to List** button.
- Step 5** To commit the changes, select the **Add** button
- Step 6** To delete an IP address(es), select the IP address in the list and then select the **Delete from List** button

Note

Multiple IP addresses may be deleted at once by making multiple selections in the list

SBC Connectivity

To open the *Connectivity* page, click the **Connectivity** button.

The *Device Details* section of the page displays the following:

- **Device Type:** This field is read only
- **Device Name:** This field is read only

The *Connected Devices* section of the page displays the following information:

- **Name:** The name of the Device
- **Type:** Indicates the type of Device
- **Description:** Description of the Device

Selecting the *Manage* link will launch the *Manage Connectivity* page.

To add connectivity, see: [Add Connectivity on page 462](#).

To manage SBC, see: [Manage Session Border Controller on page 455](#).

Procedure

View SBC Connectivity

Follow these steps to view an SBCs connectivity:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the **name** of the SBC (active text link) that you would like to manage
- Step 3** Select the **Connectivity** button

The following information will be displayed:

Field	Description
<i>Device Type</i>	This field is read only and specifies the type of device

Field	Description
<i>Device Name</i>	This field is read only and is the name of the device
<i>Name</i>	The name of the Device
<i>Type</i>	Indicates the type of Device
<i>Description</i>	Description of the Device

Note

Selecting the *Manage* link will launch the Manage Connectivity page.

Add Connectivity

The *Add Connectivity* page is launched by clicking the **Add Connectivity** button.

The *SBC Details* section of the page displays the following information:

- **Device Name:** This field is read only
- **Device Type:** This field is read only

The *SBC Connection Details* section of the page displays the following information:

- **Device Type:** This field is read only
- **Select Device:** Available unconnected Transit Switches
- **Default Port number:** Value will be used to pre-populate the interface ports on the **next** screen

The *SBC Interface Selection* section of the page displays the following information (First Phase):

- Available Interface IP addresses

Select the appropriate interfaces that will connect the transit switch with the SBC and click the **Next** button. The second provisioning screen will open.

The *SBC Interface Selection* section of the page displays the following information (Second Phase):

- **IP Address:** Selected IP Addresses from 1st phase
- **Port:** Port number to be used by the transit switch, pre-populated from the 1st phase.
- **Priority:** The ordering and priority of the interfaces, default of 1.

Clicking the **Add** button will create the connection to the transit switch.

Procedure

Adding Connectivity

Follow these steps to add connectivity for an SBC:

- Step 1** Browse to *Network > Session Border Controllers*
- Step 2** Select the **name** of the SBC (active text link) that you would like to manage
- Step 3** Select the **Connectivity** button

- Step 4** Select the **Add Connectivity** button
- Step 5** Complete all of the required fields and select the **Next** button, after completing the fields on the second page, select the **Add** button.

The connection to the transit switch will be created.

The following fields are available:

Field	Description
<i>(Connect) Device Type</i>	This field is read only
<i>Select Device</i>	Available unconnected Transit Switches
<i>Default Port number</i>	Value will be used to pre-populate the interface ports on the next screen
<i>Available Interface IP addresses</i>	This section of the screen lists all of the available IP addresses. To select an Interface, select the check-box adjacent to the relevant IP address. To select all of the available interface, select the Select all button. To clear all interface selections, select the Deselect all button.
<i>Port</i>	Port number to be used by the transit switch, pre-populated from the 1st phase.
<i>Priority</i>	The ordering and priority of the interfaces, default of 1

Allocating Location to the Hardware

Once the hardware is setup and connected to a transit, it can be associated to an unmanaged location. The association is created at the location level by browsing to *Location Administration > Telephony > SIP Device*. Here you can select from SBCs in the system and this will initiate the transaction *ActivateSBCUnmanagedLocation* which will load any required configuration into the transit based on the PGW model name *ActivateSBCUnmanagedLocation*.

Note

If the site already has a legacy gateway activated, you cannot activate an SBC connection.

SBC and OCS Management

The SBC status and OCS numbering is managed via the *SIP Devices* page. This page is accessed by browsing to *Location Administration > Telephony > SIP Devices*.

The Location Details section of the screen displays the Location ID and the Call Limit while the SBC Details section displays the selected SBC and the status of OCS Numbering.

Note

The fields and actions available on this page will change depending on the activation status of the SBC.

Activating an SBC

Note

This option will only be available if the SBC has not yet been activated.

Procedure

Follow these steps to activate an SBC:

Step 1 Browse to *Location Administration > Telephony > SIP Devices* .

Note

Dependent on your current position within the system, you may need to browse to the relevant hierarchy.

Step 2 Specify the required **Call Limit** , this is a mandatory field.

Step 3 Select the required SBC from the drop-down list.

Step 4 Specify whether you would like to activate OCS numbering by selecting the **OCSnumbering Enabled** checkbox.

Step 5 Click the **Activate** button. The SBC will now be enabled. The SIP Devices page will be updated and you will now be able to modify the SBC and deactivate it.

Deactivating an SBC

Note

- The SBC cannot be deactivated while OCS Numbering is active. Once OCS Numbering has been deactivated, the SBC can be deactivated.
 - This option will only be available if you have already activated an SBC.
-

Procedure

To deactivate an SBC:

Step 1 Browse to *Location Administration > Telephony > SIP Devices* .

Note

Dependent on your current position within the system, you may need to browse to the relevant hierarchy.

Step 2 Click the **Deactivate** button. This will deactivate the SBC.

Modifying the Call Limit and OCS Numbering

Note

This option will only be available if the SBC has already been activated.

Procedure

To manage the call limit and OCS numbering:

Step 1 Browse to *Location Administration > Telephony > SIP Devices* .

Note

Dependent on your current position within the system, you may need to browse to the relevant hierarchy.

- Step 2** Specify the *Call Limit* .
- Step 3** Select or deselect the *OCNumbering Enabled* checkbox.
- Step 4** Click the **Modify SBC** button. The SBC will be updated with your changes.

Access Profiles

Access profiles are used to manage a user's access to various features and functions within the system. Access Profiles enable System Administrators to enforce more granular control over the access to features within the predefined security roles. Access Profiles consist of a list of permission groups. A permission group governs a user's access to the associated area in the GUI as well as which transaction request actions the user may schedule from any of the other interfaces, for example bulk loaders.

Predefined security roles include (from highest to lowest level):

- Internal System user (System Administrator)
- Service Provider Administrator
- Reseller Administrator
- Customer Administrator
- Division Administrator
- Location Administrator
- End User

System administrators can control the type of access each user has to features. For each feature, they are able to specify whether the user has:

- Admin (Full access)
- Read (view only)
- Add (only) - to the system
- Update (modify only) - within the system
- Delete (only) - from the system

Typical Scenario

The highest access level user (role) in an organization is the Internal System User, otherwise known as the System Administrator. The System Administrator has the ability to manage the entire system.

The System Administrator creates the various access levels required by the lower level administrators within the organization. Each administrator can then assign the required access level to any administrator at a lower level in the hierarchy.

For example, a System Administrator may want to create different access profiles for two different Location Administrators. One access profile that allows the Location Administrator to add and

delete users, and the other that allows a more junior Location Administrator only to view (read) and update users.

In this scenario, the first access profile would have the *Add* and *Delete* options selected, and the second would have just the *Read* and *Update* options selected. These access profiles would then be assigned to the relevant administrators and could even be reused if there were similar administrator needs in other locations.

Permission Groups

Permission groups are defined for a specific GUI area and typically relate to specific menu items. It also contains the associated request actions which would typically be scheduled from that menu area. When viewing permission groups associated with an access profile, the menu area it applies to is visible in the column marked as displaying the affected area. In certain instances however, finer granularity of control is required for request actions than can be provided by the GUI structure. These can be identified in access profiles as the items where no information is available in the affected area column.

Finer granularity is required when configuring hardware elements at the network level. The following permission groups exist to control access to the request actions required to manage them.

Examples of these include:

- NetHardwareCCM. Network actions for CCM shared roles
- NetHardwareCUC. Network actions for CUC shared roles
- NetHardwareIPUnity. Network actions for IPUnity shared roles
- NetHardwareTechnician. Network actions for Technician shared roles

The above permission groups control request actions that are shared by different GUI menu areas, because the underlying hardware can be configured for different roles in order to perform different tasks. For example a Cisco Unified Communications Manager (Unified CM) can be configured as an IPPBX, Conference Server and/or Media Termination Point, to name just a few. All request actions relating to the management of a Unified CM is therefore controlled through a separate permission group, namely NetHardwareCCM. An administrator responsible for managing a Unified CM as an IPPBX from the system GUI would require the NetIPPBX permission group to gain access to the GUI area, but would also require the NetHardwareCCM permission group in order to schedule any request actions.

In contrast to this, from the *Network > PBX Devices* menu area, it is also possible to set up a general purpose IPPBX product. A system administrator does not require any other permission group other than NetIPPBX to configure this network element as it does not have multiple potential roles and the request actions are all associated to NetIPPBX.

Hardware defined in the system supporting multiple roles:

- IOSDevice
- CallManager
- IPUnity
- Unity Connection
- Technician

The management of network element attributes is controlled by the *NetHardwareAttributes* permission group. The request actions associated with this permission group is used to manage the attributes for different hardware.

An administrator would require the *NetConnect* permission group for creating connections between network elements. Transactions for creating the connection can be initiated from different GUI areas.

Exclusions

The request action scheduled by a user when changing their own password, *ChangePwd*, is not controlled by any permission group. The system allows the request action to be scheduled, but the backend transaction validates the operations allowed according to the user's associated security profile.

Note

The *SelfPassword* permission group is used only to control visibility of the Self Care Password menu item through the Read permission. A security profile setting, *Prevent user changing their own password*, also affects the behaviour of the Self Care Password menu item. If enabled, the Password menu item in Self Care is hidden. See also [Adding a security profile on page 490](#).

Managing Access Profiles

It is important for existing access profiles to be revisited after every upgrade to ensure that the correct permissions have been set for new permission groups introduced to support new features.

Note

- Only an Internal System User (System Administrator) can add, modify, or delete an access profile.
 - Any administrator can assign a specific access profile to an administrator user at a lower level.
-

Additional Restrictions

A System Administrator may configure some Providers so that the Provider's customers can manage/support their own Locations, Devices, Users, and so on, via the Admin GUI. However to ensure that the required level of security is maintained, they need to impose certain limitations/restrictions on these external administrator users.

Note

Provider administrators do not have access to the *Access Profiles* menu, so will not have knowledge of a Customer Administrator's accessibility.

This is done by selecting the *Additional Restrictions* checkbox on the *Access Profiles* screen for the required Access Profile.

This effectively disables certain functionality in selected areas of the GUI by disabling the following fields/buttons:

Procedure

End User Admin

- Step 1** Browse to *Location Administration > End User*.

- Step 2** Select an end user by clicking the required *Username* (active text link) on the *User Management* screen. The following fields are disabled on the *User Management* screen:
- Security profile
 - Feature group
 - Access profile
 - Feature display policy
 - Allow Control of Device from CTI
-

Procedure

Phone Management

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select a phone by clicking the required *Device Name* (active text link). The following fields/buttons are disabled on the *Phone Management* screen:
- SRST
 - Line Mask
 - Call waiting busy trigger
 - Max calls waiting
 - The **Add Line(s)** button
 - The **Delete Line(s)** button
-

Procedure

Extension Mobility Profile Management

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select an end user by clicking the required *Username* (active text link).
- Step 3** Click the **Extension Mobility Profile** button. The following fields/buttons are disabled on the *Manage Extension Mobility Profile* screen:
- Line mask
 - Call waiting busy trigger
 - Max calls waiting
 - The **Add Line(s)** button
 - The **Delete Line(s)** button
-

Procedure

CTI Port Management

- Step 1** Browse to *Location Administration > Telephony*.

-
- Step 2** Click the *CTI Management* (active text link).
- Step 3** Click the *CTI Ports* active text link.
- Step 4** Select the required CTI port by clicking the required *Device Name* (active text link). The following fields are disabled on the *CTI Ports Management* screen:
- Line mask
 - Call waiting busy trigger
 - Max calls waiting
-

Procedure

CTI Route Point Management

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Click the *CTI Management* (active text link).
- Step 3** Click the *CTI Route Points* active text link.
- Step 4** Select the required CTI route point by clicking the required *Device Name* (active text link). The following fields are disabled on the *CTI Route Points Management* screen:
- Line mask
 - Call waiting busy trigger
 - Max calls waiting
-

Procedure

Analog Line Management

- Step 1** Browse to *Location Administration > Analog Line Mgt.*
- Step 2** Select the required SCCP or MGCP Gateway by clicking the required *Gateway Name* (active text link). The following fields are disabled on the *Analog Port Management* screen:
- Line mask
 - Call waiting busy trigger
 - Max calls waiting
-

Limitations on Additional Restrictions

Bulk Loading and Web Services

Additional Restrictions is only effective at restricting GUI items. This means that a user can bypass these restrictions by using bulk loaders or the Web services API.

The Provider Administrator must ensure that the relevant Customer can not access Web Services by making sure that the *Web service access* checkbox is not selected on the User Management screen under *General Administration > Administrator Users*. Similarly, Bulk Loading permissions

for the user must be controlled by modifying the type of access granted to the user in the *DeploymentTools* permission group under *Setup Tools > Access Profiles*.

Add Actions

Additional restrictions are not enforced on any Add action. The provider administrator must manage the user's access profile to ensure that users do not have the access rights to add items for the following GUI areas:

- Users
- Phones
- User Mobility
- CTI Route Points
- CTI Ports
- Analog Line Management

Adding an Access Profile

Procedure

To add an Access Profile:

- Step 1** Browse to *Setup Tools > Access Profiles*.
- Step 2** Click the **Add** button.
- Step 3** Enter the required *Name* (mandatory field) and *Description* for the Access Profile.
- Step 4** Select the *Role* for the user, the options include:
- Internal system user (System Administrator)
 - Service Provider Administrator
 - Reseller Administrator
 - Customer Administrator
 - Division Administrator
 - Location Administrator
 - End User
- Step 5** Click the **Next** button. The *Add Access Profile* screen is displayed. Information on this screen is provided under the following headings:

Column	Description
Details	Name of the feature (permission group).
Description	Description of the feature.
Area Affected	Location within the system menu structure that is affected.
Admin	Select this checkbox if you would like the access profile to give the user full access (all rights) for this feature.
Read	Select this checkbox if you would like the access profile to give the user Read rights only for this feature.

Column	Description
Add	Select this checkbox if you would like the access profile to give the user Add rights only for this feature.
Update	Select this checkbox if you would like the access profile to give the user Update rights only for this feature.
Delete	Select this checkbox if you would like the access profile to give the user Delete rights only for this feature.

- Step 6** Select the Additional Restrictions checkbox (available only for Customer Administrator and lower roles) if you want to impose additional restrictions on the selected user. See [Additional Restrictions on page 467](#) for more information if required.
- Step 7** Select the required checkboxes to determine exactly what can be viewed / managed by the users associated to this access profile. The following table (see [Available Permission Groups / Access Profiles on page 471](#)), provides a direct mapping between the menus and sub-menus available in the Admin and Self Care GUIs, as well as the default setting for each of the associated access profile/permission groups (options). This is a comprehensive list of all the options available, and indicates which permission group has access to each option. Note that the displayed options depend on the user role selected.
- Step 8** Click the **Add** button. The Access Profile is added to the system.

See also: [Defaults for Access Profiles on page 475](#).

Available Permission Groups / Access Profiles

Legend:

- S = Internal system user (System Administrator)
- P = Service Provider Administrator
- R = Reseller Administrator
- C = Customer Administrator
- D = Division Administrator
- L = Location Administrator
- E = End User

Setup Tools	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Global Settings	GlobalSettings	Y	Y	Y	Y	Y	Y	N
Images	Images	Y	N	N	N	N	N	N
Branding	Branding	Y	N	N	N	N	N	N
Self Care Themes	Themes	Y	N	N	N	N	N	N
Phone Types	PhoneTypes	Y	N	N	N	N	N	N
Button Groups	ButtonGroups	Y	Y	N	N	N	N	N
Service Types	ServiceTypes	Y	N	N	N	N	N	N
Access Profiles	AccessProfiles	Y	N	N	N	N	N	N
Directory Partitions	DirectoryPartitions	Y	Y	Y	N	N	N	N
Eventing	VOSS Eventing	Y	N	N	N	N	N	N
Feature Display Policies	FeatureDisplayPolicy	Y	N	N	N	N	N	N

Setup Tools	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Audit	VOSSAudit	Y	N	N	N	N	N	N
Bulk Load Samples	Samples	Y	Y	Y	Y	Y	Y	N
Security Profiles	ApplicationSecurity	Y	N	N	N	N	N	N

Dial Plan Tools	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Number Construction	NumberRules	Y	N	N	N	N	N	N
Hardware Sets	HardwareSets	Y	N	N	N	N	N	N
Configuration Models	ProductModels	Y	N	N	N	N	N	N
Countries	Countries	Y	Y	N	N	N	N	N
Model Management	ManageCCMModel	Y	N	N	N	N	N	N
Migrate Models	MigrateModels	Y	N	N	N	N	N	N

Provider Administrator	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Providers	Provider	Y	N	N	N	N	N	N
Provider Countries	ProviderCountries	Y	Y	N	N	N	N	N
Feature Group Templates	FeatureGroupTemplates	Y	Y	N	N	N	N	N
PBX Templates	PBXTemplates	Y	N	N	N	N	N	N

Network	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
IOS Devices	NetIOSDevice	Y	Y	Y	Y	Y	Y	N
Gatekeepers	NetGatekeeper	Y	Y	N	N	N	N	N
Transit Switches	NetTransit	Y	Y	N	N	N	N	N
PBX Devices	NetIPPBX	Y	Y	N	N	N	N	N
DHCP Servers	NetDHCP	Y	Y	N	N	N	N	N
TFTP Servers	NetTFTP	Y	Y	N	N	N	N	N
Voicemail Gateways	NetVMGateway	Y	Y	N	N	N	N	N
IP Edge Devices	NetIPEdge	Y	Y	N	N	N	N	N
Console Servers	NetConsole	Y	Y	N	N	N	N	N
Music Servers	NetMusic	Y	Y	N	N	N	N	N
Conference Servers	NetConference	Y	Y	N	N	N	N	N
Transcoder Servers	NetTranscoder	Y	Y	N	N	N	N	N
Annunciator Servers	NetAnnunciator	Y	Y	N	N	N	N	N
Media Termination Point	NetMTP	Y	Y	N	N	N	N	N
Voicemail Servers	NetVoicemail	Y	Y	N	N	N	N	N
Directory Servers	NetDirectory	Y	Y	N	N	N	N	N
Emergency Responder	NetEResponder	Y	Y	N	N	N	N	N
Presence Servers	NetPresence	Y	Y	N	N	N	N	N
IVR Servers	NetIVR	Y	Y	N	N	N	N	N
SIP Application Servers	NetSIPServer	Y	Y	Y	Y	Y	Y	N

Network	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Hardware Groups	NetHardwareGroup	Y	Y	N	N	N	N	N
Session Border Controllers	NetSBC	Y	Y	N	N	N	N	N
Contact Center Servers	NetContactCentre	Y	Y	N	N	N	N	N
Authentication Servers	AuthMgt	Y	Y	Y	Y	Y	Y	N

Resources	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
E164 Inventory	ResourceE164	Y	Y	N	N	N	N	N
Authorization Codes	ResourceAuthCode	Y	Y	Y	Y	Y	Y	Y
Billing Codes	ResourceBillingRef	Y	Y	Y	Y	Y	Y	Y
Managed IP Subnets	ResourceIPAddress	Y	Y	N	N	N	N	N
Site Code Inventory	ResourceSiteCode	Y	Y	N	N	N	N	N
Voicemail Services	ResourceVMServices	Y	Y	N	N	N	N	N
Auto Attendant Services	ResourceAAServices	Y	Y	Y	Y	Y	N	N
Console Services	ResourceConsoleServices	Y	Y	N	N	N	N	N
Directory Services	ResourceDirectoryServices	Y	Y	N	N	N	N	N
Conference Services	ResourceConferenceServices	Y	Y	Y	N	N	N	N
Media Services	ResourceMediaServices	Y	Y	N	N	N	N	N
Phone Inventory	ResourcePhones	Y	Y	Y	Y	Y	Y	N
Contact Center Service	ResourceContactCentreService	Y	Y	N	N	N	N	N
MoH Tracks	ResourceMOHTrackMgt	Y	Y	Y	Y	Y	Y	N
SMTP Server	CustomererrSMTP	Y	Y	Y	Y	N	N	N

General Tools	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Operations Tools	OpsTools	Y	Y	N	N	N	N	N
Bulk Load Tools	DeploymentTools	Y	Y	Y	Y	Y	Y	N
Transactions	Transactions	Y	Y	Y	Y	Y	Y	N
Bulk Administration	DeploymentTools	Y	Y	Y	Y	Y	Y	N

General Administration	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Administration Users	Users	Y	Y	Y	Y	Y	Y	N
Resellers	Resellers	Y	Y	N	N	N	N	N
Buildings	Buildings	Y	Y	Y	N	N	N	N
CLI Groups	CLIGroups	Y	Y	Y	Y	Y	Y	N
Customers	Customers	Y	Y	Y	N	N	N	N
Divisions	Divisions	Y	Y	Y	Y	N	N	N
Locations	Locations	Y	Y	Y	Y	Y	N	N
Feature Groups	FeatureGroups	Y	Y	Y	Y	N	N	N
Number Translation	NumberTranslation	Y	Y	Y	Y	Y	Y	N

General Administration	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Feature Configuration Templates	FeatureConfigTemplate	Y	Y	Y	Y	N	N	N
End User Migration	UserMigration	Y	Y	N	N	N	N	N

Location Administration	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Switchboards	LocationConsole	Y	Y	Y	Y	Y	Y	N
Telephony	LocationTelephony	Y	Y	Y	Y	Y	Y	N
Hunt Groups	LocationHuntGroups	Y	Y	Y	Y	Y	Y	N
Number Groups	LocationNumberGroups	Y	Y	Y	Y	Y	Y	N
Pickup Groups	LocationPickupGroups	Y	Y	Y	Y	Y	Y	N
End Users	LocationUsers	Y	Y	Y	Y	Y	Y	N
Phone Inventory	LocationPhones	Y	Y	Y	Y	Y	Y	N
Phone Registration	LocationPhoneReg	Y	Y	Y	Y	Y	Y	N
Phone Management	LocationPhoneAdmin	Y	Y	Y	Y	Y	Y	N
Analog Line Mgt.	LocationAnalogueLineMgt	Y	Y	Y	Y	Y	Y	N
Internal Numbers	LocationExtensions	Y	Y	Y	Y	Y	Y	N
External Numbers	LocationE164	Y	Y	Y	Y	Y	Y	N
Administration Tools	LocationAdminTools	Y	Y	Y	Y	Y	Y	N

My Account	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Account Settings	AccountMgt	Y	Y	Y	Y	Y	Y	N

Self Care	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
Note This section is relevant only to the menu items available to Self Care End Users, and is not relevant to any of the other administrator levels.								
Conferencing	SelfConference	N	N	N	N	N	N	Y
Details	SelfDetails	N	N	N	N	N	N	Y
Corporate Directory	SelfDirectory	N	N	N	N	N	N	Y
Mobile Identity	SelfMobileIdentity	N	N	N	N	N	N	Y
Password	SelfPassword	N	N	N	N	N	N	Y
Personal Directory	SelfPersonalDir	N	N	N	N	N	N	Y
Phone PIN	SelfPhonePin	N	N	N	N	N	N	Y
My Phones	SelfPhones	N	N	N	N	N	N	Y
My Preferences	SelfPreferences	N	N	N	N	N	N	Y
Presence	SelfPresence	N	N	N	N	N	N	Y
Extension Mobility	SelfRoaming	N	N	N	N	N	N	Y
Single Number Reach	SelfSNR	N	N	N	N	N	N	Y
My Transactions	SelfTransactions	N	N	N	N	N	N	Y

Self Care	Related Permission Group	Available to (Administrator/End User)						
		S	P	R	C	D	L	E
UC Central	SelfUCCentral	N	N	N	N	N	N	Y
Voicemail	SelfVoiceMail	N	N	N	N	N	N	Y

Modifying and Deleting Access Profiles

Procedure

Modifying an Access Profile

To modify an Access Profile:

- Step 1** Browse to *Setup Tools > Access Profiles*.
- Step 2** Select the *Name* (active text link) of the Access Profile that you would like to modify.
- Step 3** Select the *Additional Restrictions* checkbox (available only for Customer Administrator and lower roles) if you want to impose additional restrictions on the selected user. See [Additional Restrictions on page 467](#) for more information if required.
- Step 4** Modify the options that you would like the user to be able to access, by selecting or deselecting the appropriate checkboxes to determine the level of access. See [Available Permission Groups / Access Profiles on page 471](#) for a comprehensive list of the available options.
- Step 5** Click the **Modify** button when complete to save your changes. The Access Profile is updated within the system.

Note

- New permissions are not added to existing access profiles during the upgrade procedure. New permissions are shown in an existing access profile with a reference marker (*). This means that the user would have the permission settings inherited from the default permissions set on the user's role. If the access profile is "Modified", the new permissions are saved to the access profile according to the selected control settings.

Procedure

Deleting an Access Profile

To delete an Access Profile:

- Step 1** Browse to *Setup Tools > Access Profiles*.
- Step 2** Select the *Name* (active text link) of the Access Profile that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the Access Profile is removed from the system.

Defaults for Access Profiles

The following lists indicate the default role permissions for each type of user. This governs a user's actions according to the user's role if the user's access profile setting is set to default.

Internal System Super User (System Administrator)

The following default access profiles are available for Internal System Super Users:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccessProfiles	Access profile management	Y	Y	Y	Y	Y
AccountMgt	My account management	Y	Y	Y	Y	Y
ApplicationSecurity	Security	Y	Y	Y	Y	Y
AuthMgt	Auth management	Y	Y	Y	Y	Y
Branding	Branding management	Y	Y	Y	Y	Y
Buildings	Building management	Y	Y	Y	Y	Y
ButtonGroups	Button group management	Y	Y	Y	Y	Y
CLIGroups	CLI group management	Y	Y	Y	Y	Y
Countries	Countries per Provider management	Y	Y	Y	Y	Y
Customers	Customer management	Y	Y	N	Y	N
CustomerSMTP	Customer SMTP management	Y	Y	Y	Y	Y
DeploymentTools	Deployment tools	Y	Y	Y	Y	Y
DirectoryPartitions	Directory partition management	Y	Y	Y	Y	Y
Divisions	Division management	Y	Y	Y	Y	Y
ExtensionMobilityLocation-Group	Network actions for Extension Mobility Location Group roles	Y	Y	Y	Y	Y
FeatureConfigTemplate	Feature Configuration Template management	Y	Y	Y	Y	Y
FeatureDisplayPolicy	Feature display policy management	Y	Y	Y	Y	Y
FeatureGroups	Feature groups	Y	Y	Y	Y	Y
FeatureGroupTemplates	Feature group management	Y	Y	Y	Y	Y
GlobalSettings	Global settings	Y	Y	Y	Y	Y
HardwareSets	Hardware set management	Y	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogueLineMgt	Location Analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location Switchboard management	Y	Y	Y	Y	Y
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN Number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumberGroups	Location number group management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pickup group management	Y	Y	Y	Y	Y
Locations	Location management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
ManageCCMModel	Model management	Y	Y	Y	Y	Y
MigrateModels	Model migration management	Y	Y	Y	Y	Y
NetAnnunciator	Network announcement server management	Y	Y	Y	Y	Y
NetConference	Network conference management	Y	Y	Y	Y	Y
NetConnect	Network interconnect transactions	Y	Y	Y	Y	Y
NetConsole	Network console management	Y	Y	Y	Y	Y
NetContactCenter	Contact Center	Y	Y	Y	Y	Y
NetDHCP	Network DHCP management	Y	Y	Y	Y	Y
NetDirectory	Network directory management	Y	Y	Y	Y	Y
NetEResponder	Network emergency responder management	Y	Y	Y	Y	Y
NetGateKeeper	Network gatekeeper management	Y	Y	Y	Y	Y
NetHardwareAttributes	Network hardware attribute management	Y	Y	Y	Y	Y
NetHardwareCCM	Network actions for CCM shared roles	Y	Y	Y	Y	Y
NetHardwareCUC	Network actions for CUC shared roles	Y	Y	Y	Y	Y
NetHardwareGroup	Hardware group management	Y	Y	Y	Y	Y
NetHardwareIPUnity	Network actions for IPUnity shared roles	Y	Y	Y	Y	Y
NetHardwareTechnician	Network actions for Technician shared roles	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	Y	Y	Y	Y	Y
NetIPEdge	Network IP edge management	Y	Y	Y	Y	Y
NetIPPBX	Network IP PBX management	Y	Y	Y	Y	Y
NetIVR	Network IVR management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
NetMTP	Network media termination point management	Y	Y	Y	Y	Y
NetMusic	Network music management	Y	Y	Y	Y	Y
NetSBC	Network SBC management	Y	Y	Y	Y	Y
NetSIPServer	Network SIP server management	Y	Y	Y	Y	Y
NetTFTP	Network TFTP management	Y	Y	Y	Y	Y
NetTranscoder	Network transcoder management	Y	Y	Y	Y	Y
NetTransit	Network transit management	Y	Y	Y	Y	Y
NetVMGateway	Network Voicemail gateway management	Y	Y	Y	Y	Y
NetVoiceMail	Network Voicemail management	Y	Y	Y	Y	Y
NumberRules	Number construction tools	Y	Y	Y	Y	Y
NumberTranslation	Number translation management	Y	Y	Y	Y	Y
OpsTools	Operations tools	Y	Y	Y	Y	Y
PBXTemplates	PBX template management	Y	Y	Y	Y	Y
PhoneTypes	Phone type management	Y	Y	Y	Y	Y
Presence	Group for CUPS server management	Y	Y	Y	Y	Y
ProductModels	Product models	Y	Y	Y	Y	Y
Provider	Provider administration	Y	Y	Y	Y	Y
ProviderCountries	Provider countries	Y	Y	Y	Y	Y
Resellers	Reseller management	Y	Y	Y	Y	Y
ResourceAAServices	Auto attendant services management	Y	Y	Y	Y	Y
ResourceAuthCode	Authorization code management	Y	Y	Y	Y	Y
ResourceBillingRef	Billing reference inventory management	Y	Y	Y	Y	Y
ResourceConferenceServices	Conference services management	Y	Y	Y	Y	Y
ResourceConsoleServices	Console services management	Y	Y	Y	Y	Y
ResourceContactCenterService	Contact Center service	Y	Y	Y	Y	Y
ResourceDirectoryServices	Directory services management	Y	Y	Y	Y	Y
ResourceE164	E164 inventory management	Y	Y	Y	Y	Y
ResourceIPAddress	IPAddress inventory management	Y	Y	Y	Y	Y
ResourceMediaServices	Media services management	Y	Y	Y	Y	Y
ResourceMOHTrackMgt	Location Music management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
ResourcePhones	Phone inventory management	Y	Y	Y	Y	Y
ResourceSiteCode	Site code inventory management	Y	Y	Y	Y	Y
ResourceVMServices	Voicemail services management	Y	Y	Y	Y	Y
Samples	Sample data	Y	Y	Y	Y	Y
SelfConference	Self Care Conference	Y	Y	Y	Y	Y
SelfDetails	Self Care basic management	Y	Y	Y	Y	Y
SelfDirectory	Corporate Directory	Y	Y	Y	Y	Y
SelfMobileIdentity	Self Care Mobile Identity	Y	Y	Y	Y	Y
SelfPassword	Self Care Password management	Y	Y	Y	Y	Y
SelfPersonalDir	Personal Directory	Y	Y	Y	Y	Y
SelfPhonePin	SelfCare Phone Pin	Y	Y	Y	Y	Y
SelfPhones	SelfCare Phone management	Y	Y	Y	Y	Y
SelfPreferences	Self Care Preferences	Y	Y	Y	Y	Y
SelfPresence	Self-Care Presence	Y	Y	Y	Y	Y
SelfRoaming	Self Care Roaming management	Y	Y	Y	Y	Y
SelfSNR	Single Number Reach for users	Y	Y	Y	Y	Y
SelfTransactions	SelfCare Transactions	Y	Y	Y	Y	Y
SelfUCCentral	Self Care UC Central	Y	Y	Y	Y	Y
SelfVoiceMail	Personal Voicemail management	Y	Y	Y	Y	Y
ServiceTypes	Service type management	Y	Y	Y	Y	Y
Themes	Theme management	Y	Y	Y	Y	Y
Transactions	Transaction tools	Y	Y	Y	Y	Y
UserMigration	Users and device migration	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y
VOSSAudit	Audit application management	Y	Y	Y	Y	Y
VOSSEventing	Eventing management	Y	Y	Y	Y	Y

Service Provider Administrators

The following default access profiles are available for Service Provider Administrators:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccountMgt	My account management	Y	Y	Y	Y	Y
AuthMgt	Auth management	Y	Y	Y	Y	Y
Buildings	Building management	Y	Y	Y	Y	Y
ButtonGroups	Button Group management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
CLIGroups	CLI group management	Y	Y	Y	Y	Y
Countries	Countries per provider management	N	Y	Y	Y	Y
Customers	Customer management	Y	Y	Y	Y	Y
CustomerSMTP	Customer SMTP management	Y	Y	Y	Y	Y
DeploymentTools	Deployment tools	Y	Y	Y	Y	Y
DirectoryPartitions	Directory partition management	Y	Y	Y	Y	Y
Divisions	Division management	Y	Y	Y	Y	Y
ExtensionMobilityLocation-Group	Network actions for Extension Mobility Location Group roles	Y	Y	Y	Y	Y
FeatureConfigTemplate	Feature Configuration Template management	Y	Y	Y	Y	Y
FeatureGroups	Feature groups	Y	Y	Y	Y	Y
FeatureGroupTemplates	Feature group management	Y	Y	Y	Y	Y
GlobalSettings	Global settings	Y	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogueLineMgt	Location analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location switchboard management	Y	Y	Y	Y	Y
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumberGroups	Location number group management	Y	Y	Y	Y	Y
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pickup group management	Y	Y	Y	Y	Y
Locations	Location management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
NetAnnunciator	Network announcement server management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
NetConference	Network conference management	Y	Y	Y	Y	Y
NetConnect	Network interconnect transactions	Y	Y	Y	Y	Y
NetConsole	Network console management	Y	Y	Y	Y	Y
NetContactCenter	Contact Center	Y	Y	Y	Y	Y
NetDHCP	Network DHCP management	Y	Y	Y	Y	Y
NetDirectory	Network directory management	Y	Y	Y	Y	Y
NetEResponder	Network emergency responder management	Y	Y	Y	Y	Y
NetGateKeeper	Network gatekeeper management	Y	Y	Y	Y	Y
NetHardwareAttributes	Network hardware attribute management	Y	Y	Y	Y	Y
NetHardwareCCM	Network actions for CCM shared roles	Y	Y	Y	Y	Y
NetHardwareCUC	Network actions for CUC shared roles	Y	Y	Y	Y	Y
NetHardwareGroup	Hardware group management	Y	Y	Y	Y	Y
NetHardwareIPUnity	Network actions for IPUnity shared roles	Y	Y	Y	Y	Y
NetHardwareTechnician	Network actions for technician shared roles	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	Y	Y	Y	Y	Y
NetIPEdge	Network IP edge management	Y	Y	Y	Y	Y
NetIPPBX	Network IP PBX management	Y	Y	Y	Y	Y
NetIVR	Network IVR management	Y	Y	Y	Y	Y
NetMTP	Network media termination point management	Y	Y	Y	Y	Y
NetMusic	Network music management	Y	Y	Y	Y	Y
NetSBC	Network SBC management	Y	Y	Y	Y	Y
NetSIPServer	Network SIP server management	Y	Y	Y	Y	Y
NetTFTP	Network TFTP management	Y	Y	Y	Y	Y
NetTranscoder	Network transcoder management	Y	Y	Y	Y	Y
NetTransit	Network transit management	Y	Y	Y	Y	Y
NetVMGateway	Network Voicemail gateway management	Y	Y	Y	Y	Y
NetVoiceMail	Network Voicemail management	Y	Y	Y	Y	Y
NumberTranslation	Number Translation management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
OpsTools	Operations tools	Y	Y	Y	Y	Y
Presence	Group for CUPS server management	Y	Y	Y	Y	Y
ProviderCountries	Provider countries	Y	Y	Y	Y	Y
Resellers	Reseller management	Y	Y	Y	Y	Y
ResourceAAServices	Auto attendant services management	Y	Y	Y	Y	Y
ResourceAuthCode	Authorization code management	Y	Y	Y	Y	Y
ResourceBillingRef	Billing reference inventory management	Y	Y	Y	Y	Y
ResourceConferenceServices	Conference services management	Y	Y	Y	Y	Y
ResourceConsoleServices	Console services management	Y	Y	Y	Y	Y
ResourceContactCenterService	Contact Center service	Y	Y	Y	Y	Y
ResourceDirectoryServices	Directory services management	Y	Y	Y	Y	Y
ResourceE164	E164 inventory management	Y	Y	Y	Y	Y
ResourceIPAddress	IPAddress inventory management	Y	Y	Y	Y	Y
ResourceMediaServices	Media services management	Y	Y	Y	Y	Y
ResourceMOHTrackMgt	Location Music management	Y	Y	Y	Y	Y
ResourcePhones	Phone inventory management	Y	Y	Y	Y	Y
ResourceSiteCode	Site code inventory management	Y	Y	Y	Y	Y
ResourceVMServices	Voicemail services management	Y	Y	Y	Y	Y
Samples	Sample data	N	Y	N	N	N
Transactions	Transaction tools	Y	Y	Y	Y	Y
UserMigration	Users and device migration	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y

Reseller Administrator

The following default access profiles are available for Reseller Administrators:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccountMgt	My account management	Y	Y	Y	Y	Y
AuthMgt	Auth management	N	N	N	N	N
Buildings	Building management	Y	Y	Y	Y	Y
CLIGroups	CLI group management	Y	Y	Y	Y	Y
Customers	Customer management	Y	Y	Y	Y	Y
CustomerSMTP	Customer SMTP management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
DeploymentTools	Deployment Tools	Y	Y	Y	Y	Y
DirectoryPartitions	Directory partition management	Y	Y	Y	Y	Y
Divisions	Division management	Y	Y	Y	Y	Y
ExtensionMobilityLocation-Group	Network actions for Extension Mobility Location Group roles	Y	Y	Y	Y	Y
FeatureConfigTemplate	Feature Configuration Template management	Y	Y	Y	Y	Y
FeatureGroups	Feature groups	Y	Y	Y	Y	Y
GlobalSettings	Global settings	N	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogueLineMgt	Location analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location switchboard management	Y	Y	Y	Y	Y
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumberGroups	Location number group management	Y	Y	Y	Y	Y
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pickup group management	Y	Y	Y	Y	Y
Locations	Location management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	N	N	N	N	N
NumberTranslation	Number Translation Management	Y	Y	Y	Y	Y
ResourceAAServices	Auto Attendant Services management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
ResourceConferenceServices	Conference services management	Y	Y	Y	Y	Y
ResourceContactCenterService	Contact Center Service	Y	Y	Y	Y	Y
ResourceE164	E164 Inventory management	Y	Y	Y	Y	Y
ResourcePhones	Phone inventory management	N	Y	N	N	N
ResourceVMService	Voicemail Services management	Y	Y	Y	Y	Y
Samples	Sample data	N	Y	N	N	N
Transactions	Transaction tools	Y	Y	Y	Y	Y
UserMigration	Users and device migration	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y

Customer Administrators

The following default access profiles are available for Customer Administrators:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccountMgt	My account management	Y	Y	Y	Y	Y
AuthMgt	Auth management	N	N	N	N	N
CLIGroups	CLI group management	Y	Y	Y	Y	Y
CustomerSMTP	Customer SMTP management	Y	Y	Y	Y	Y
DeploymentTools	Deployment tools	Y	Y	Y	Y	Y
Divisions	Division management	Y	Y	Y	Y	Y
ExtensionMobilityLocation-Group	Network actions for Extension Mobility Location Group roles	Y	Y	Y	Y	Y
FeatureConfigTemplate	Feature Configuration Template management	Y	Y	Y	Y	Y
FeatureGroups	Feature groups	Y	Y	Y	Y	Y
GlobalSettings	Global settings	Y	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogueLineMgt	Location analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location switchboard management	Y	Y	Y	Y	Y
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumberGroups	Location number group management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pickup group management	Y	Y	Y	Y	Y
Locations	Location management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	N	N	N	N	N
NumberTranslation	Number translation management	Y	Y	Y	Y	Y
ResourceAAServices	Auto attendant services management	Y	Y	Y	Y	Y
ResourceConferenceServices	Conference Services Management	Y	Y	Y	Y	Y
ResourceContactCenterService	Contact Center Service	Y	Y	Y	Y	Y
ResourceE164	E164 Inventory management	Y	Y	Y	Y	Y
ResourcePhones	Phone inventory management	N	Y	N	N	N
ResourceVMServices	Voicemail Services management	Y	Y	Y	Y	Y
Samples	Sample data	N	Y	N	N	N
Transactions	Transaction tools	Y	Y	Y	Y	Y
UserMigration	Users and device migration	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y

Division Administrators

The following default access profiles are available for Division Administrators:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccountMgt	My account management	Y	Y	Y	Y	Y
AuthMgt	Auth management	N	N	N	N	N
CLIGroups	CLI group management	Y	Y	Y	Y	Y
DeploymentTools	Deployment tools	Y	Y	Y	Y	Y
GlobalSettings	Global settings	Y	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogueLineMgt	Location analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location switchboard management	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumberGroups	Location number group management	Y	Y	Y	Y	Y
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pickup group management	Y	Y	Y	Y	Y
Locations	Location management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	N	N	N	N	N
NumberTranslation	Number translation management	Y	Y	Y	Y	Y
ResourceAAServices	Auto attendant services management	Y	Y	Y	Y	Y
ResourceAAServices	Auto Attendant Services management	Y	Y	Y	Y	Y
ResourcePhones	Phone inventory management	N	Y	N	N	N
Samples	Sample data	N	Y	N	N	N
Transactions	Transaction tools	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y

Location Administrators

The following default access profiles are available for Location Administrators:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
AccountMgt	My account management	Y	Y	Y	Y	Y
AuthMgt	Auth management	N	N	N	N	N

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
CLIGroups	CLI group management	Y	Y	Y	Y	Y
DeploymentTools	Deployment tools	Y	Y	Y	Y	Y
GlobalSettings	Global settings	Y	Y	Y	Y	Y
LocationAdminTools	Location tools management	Y	Y	Y	Y	Y
LocationAnalogue-LineMgt	Location analog port detail management	Y	Y	Y	Y	Y
LocationConsole	Location switch-board management	Y	Y	Y	Y	Y
LocationDeviceGroups	Location device groups management	Y	Y	Y	Y	Y
LocationE164	Location PSTN number management	Y	Y	Y	Y	Y
LocationExtensions	Extension number management	Y	Y	Y	Y	Y
LocationHuntGroups	Location hunt group management	Y	Y	Y	Y	Y
LocationNumber-Groups	Location number group management	Y	Y	Y	Y	Y
LocationPhoneAdmin	Location phone detail management	Y	Y	Y	Y	Y
LocationPhoneReg	Location phone registration	Y	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
LocationPhones	Location phone inventory management	Y	Y	Y	Y	Y
LocationPickupGroups	Location pick-up group management	Y	Y	Y	Y	Y
LocationTelephony	Location telephony management	Y	Y	Y	Y	Y
LocationUsers	Location user management	Y	Y	Y	Y	Y
NetIOSDevice	Network IOS device management	N	N	N	N	N
NumberTranslation	Number translation management	Y	Y	Y	Y	Y
ResourcePhones	Phone inventory management	Y	Y	Y	Y	Y
Samples	Sample data	N	Y	N	N	N
Transactions	Transaction tools	Y	Y	Y	Y	Y
Users	User management	Y	Y	Y	Y	Y

Self Care

The following default access profiles are available for Self Care users:

Permission Group	Description	Admin (All)	Read	Add	Update	Delete
SelfConference	Self Care conference	N	Y	Y	Y	Y
SelfDetails	Self Care basic management	N	Y	Y	Y	Y
SelfDirectory	Corporate directory	N	Y	Y	Y	Y
SelfMobileIdentity	Self Care mobile identity	N	Y	Y	Y	Y
SelfPassword	Self Care password management	N	Y	Y	Y	Y
SelfPersonalDir	Personal directory	N	Y	Y	Y	Y
SelfPhonePin	Self Care phone Pin	N	Y	Y	Y	Y

Permission Group	Description	Admin (All)	Read	Add	Up-date	Delete
SelfPhones	Self Care phone management	N	Y	Y	Y	Y
SelfPreferences	Self Care preferences	N	Y	Y	Y	Y
SelfPresence	Self-Care presence	N	Y	Y	Y	Y
SelfRoaming	Self Care roaming management	N	Y	Y	Y	Y
SelfSNR	Single number reach for users	N	Y	Y	Y	Y
SelfTransactions	Self Care transactions	N	Y	Y	Y	Y
SelfUCCentral	Self Care UC Central	N	Y	Y	Y	Y
SelfVoiceMail	Personal Voicemail management	N	Y	Y	Y	Y

Security profiles

This section covers security profile management and includes adding, modifying and deleting a profile; setting defaults and profiles at the various levels as well as lockout.

Security profile management

Security profiles are sets of rules that govern password strength and other security related preferences. Security profiles can be applied at system level and at various hierarchical levels which are Provider, Reseller, Customer, Division, Location and Users. Security profile chosen at a level would be applied to all the users and objects within that level which have *not* explicitly chosen a profile. If a security profile is not defined at a level it would inherit the profile of the level above with the final fallback being the default profile of the system.

The Security profiles can be managed from *Setup Tools > Security Profiles*. The default profile for the system can also be selected from here. A default security profile called *Default* would be available in the system. Only a System administrator would be able to add/delete/modify a security profile.

Note

- A default security profile called *Default* is installed when the system is installed.
 - Only a System administrator can add, delete and modify security profiles.
-

For adding, modifying and deleting a profile, see:

- [Adding a security profile on page 490](#)
- [Modifying and deleting security profiles on page 493](#)

Setting a default security profile for the system

The default profile for the system can be set by browsing to *Setup Tools > Security Profiles*, the *Security Profile Management* screen lists all the profiles available in the system and a radio button is available under the column *System Default Profile* to set the default profile for the system.

Note

- If an administrator would like to inherit the provider security profile, the administrator would select none for the customer, location and user.

- For the system super user, they can only default to the system default.

Procedure

Setting a default security profile for the system

To set a security profile as the default security profile:

- Step 1** Navigate to *Setup Tools > Security Profiles*.
- Step 2** Select the security profile that you would like to set as default by selecting the radio button adjacent to the required security profile.
- Step 3** Click the **Update** button.
-

The security profile is set as the default security profile.

Setting security profiles at the various hierarchical levels

Security profiles can be applied to various hierarchical levels Provider, Reseller, Customer, Location and User. A drop-down list listing all the available Security Profiles in the system is available on the management screens of Provider, Reseller, Customer, Location and User for selection.

If a security profile is not selected at a level (none is selected in the options list) then the security profile of the level above is inherited with the final fallback being the default security profile of the system.

Adding a security profile

Procedure

Adding a security profile

To add a security profile:

- Step 1** Navigate to *Setup Tools > Security Profiles*.
- Step 2** Click the **Add** button.

Complete the required fields. The following settings are available when adding a security profile:

Field	Description
Details	
Profile Name	The name to be used for the security profile. This is a mandatory field.
Description	A short description for the security profile.
External Authentication	
Enable external authentication	Select the checkbox if users linked to the security profile must be authenticated via an external authentication server, for example LDAP. Note When external authentication is enabled, all authentication rules related fields are disabled as the applicable rules are managed by the external authentication server.
Security Preferences	

Field	Description
Deny Simultaneous Logins	<p>If set, the application does not allow users to have two sessions running concurrently.</p> <p>This means that simultaneous sessions from different computers, or different browsers on the same computer, are not possible. The user may however open two or more tabs in the same browser instance. In this case, no authentication is required in the second and subsequent tabs.</p> <p>Note</p> <p>If the user closes a logged-in browser session, without first logging out from the system, it is not possible to log in again until the session TTL has expired.</p>
Allow User Login without prompting to change the password/pin after reset	<p>If set, the system allows a user to login to the application or phone without prompting the user to change their password/pin at first login.</p> <p>Note</p> <p>A higher level administrator may change the password of a lower level admin or end user to a value that does not comply with the rules specified in the security profile, provided that the lower level user has permission to change their own password. The user must change a reset password immediately after logging in. Passwords set by the higher level user must comply with the password rules if the lower level user may not change their own password, or is not prompted to change their password on login - this would lead to the possibility of insecure passwords being set and retained.</p>
Prevent user changing their own password	<p>If selected, the user is not allowed to change their own password, and the Password menu item in Self Care is hidden. The password may only be updated by an administrator. See also under <i>Exclusions</i> in Access Profiles on page 465.</p>
Session TTL (seconds)	<p>The session time-out in seconds. The minimum value for this field is 120 seconds, however, the system recommends setting this to at least 300 seconds.</p>
Phone PIN Strength Rules	
Minimum length of Phone PIN	<p>This can be between 1 & 127 digits.</p>
Password Strength Rules	
Minimum Length of Password (min. 6 characters)	<p>The minimum length required for passwords is six (6) characters, the default value is 9.</p>
Password strength type	<p>Controls the level of password validation with regards to patterns and dictionary checks for the end user password in CUCDM and Self Care. The current options are: <i>High</i> (default), <i>Medium</i>, or <i>Low</i>. The minimum password length for all options is 6 characters. <i>Low</i> = no validation rules; <i>Medium</i> = medium complexity password required, in that the password must not be similar to any password used on the account within a specified amount of days, and the password must not be based on a dictionary word or sequence, for example abc, 123, or querty; <i>High</i> = Additional complexity rules are imposed and checked, that is, the password must not be a palindrome, and must include additional complexity rules as determined by the length credits field settings below.</p>

Field	Description
Minimum characters to differ from previous password	The minimum character proximity allowed to previously used passwords, the default value is 3.
Length Credits for Upper case, Lower case, Digits and Non-Alphanumeric	The minimum length of the password becomes minimum length minus the length of credits specified. If a negative value is specified, then this is the minimum number of that type of character that must appear in the password. These are mandatory fields when the <i>Password strength type</i> field (see above) is set to <i>High</i> , and must be completed.
Password Ageing	
Disable password ageing	Select this checkbox to disable the password ageing feature
Maximum password age (days)	This is the maximum lifetime (in days) of a password. When a password reaches this age, it must be changed. If left blank, the passwords do not expire.
Password expiry warning period (days)	As a password approaches the maximum age, a warning may be displayed after the user has logged in, this warns them that their password is about to expire. If left blank, no warnings are displayed.
Period for which a password may not be re-used (days)	The minimum period that must pass before an old password may be reused. If left blank, there is no minimum period.
Lock User Account on Failed Login Attempt	
Enable account locking on failed logins	<p>If selected, the system locks user accounts if the configured number of failed logins is reached. Default is blank (not selected).</p> <p>When this option is disabled, a user can attempt to login as many times as they wish without having their account locked. If this option is enabled, the account is locked after the number of login attempts threshold is breached. In order for the account to be usable again, account unlocking must be enabled, which unlocks the account if the user logs in after the time to keep locked threshold has expired. Any attempts to login during this grace period resets the last login attempt time and the user is kept locked out until a new grace period has expired.</p> <p>If the <i>Enable account unlocking</i> option (see below) is not selected (disabled), user accounts can only be unlocked by the database administrator. Unlocking only occurs if the user logs in with the correct password after the grace period has expired and if the account unlocking option is enabled. If an account needs to be unlocked before the grace period has expired or in the case where the unlock account option is disabled, only the database administrator is able to unlock the account by directly enabling the account in the database. This can be done using: <code>UPDATE person SET disabled='N' WHERE username='?';</code></p> <p>To prevent administrator users from being locked out, the types of user that can be locked out can be defined within the system. To limit the lockout functionality to certain user types, select the required user types and enable account locking. For example, if lockout should only occur for end user accounts, select only lockout end users and enable account locking (see below).</p>
Lockout System User	If selected, the system locks system user accounts if the configured number of failed logins is reached. Default is blank (not selected).

Field	Description
Lockout Provider Admin	If selected, the system locks provider administrator user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Lockout Reseller Admin	If selected, the system locks reseller administrator user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Lockout Customer Admin	If selected, the system locks customer administrator user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Lockout Division Admin	If selected, the system locks division administrator user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Lockout Location Admin	If selected, the system locks location administrator user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Lockout End User	If selected, the system locks end user accounts if the configured number of failed logins is reached. Default is blank (not selected).
Number of login attempts	This is the number of failed login attempts before the system locks the user account. For example, if configured at 3, and a user enters three incorrect passwords, the system locks the user's account. Default = 3.
Enable account unlocking	If selected, the system does not permanently lock user accounts but automatically unlocks the accounts after a pre-configured interval has transpired.
Time to keep account locked (seconds)	This is the interval between the system locking the account and the user account being automatically unlocked. Default value = 1800.

Step 3 Click the **Add** button and the security profile is added to the system.

Note

There is an absolute minimum password length of 6 characters, irrespective of the settings above. If password ageing is disabled or if the password re-use period is blank then the password must be different from the 5 most recent passwords used on that account.

Modifying and deleting security profiles

Procedure

Modifying security profiles

To modify an existing security profile:

- Step 1** Navigate to *Setup Tools > Security Profiles*.
- Step 2** Select the security profile that you would like to modify.
- Step 3** Make the required modifications and click the **Modify** button. See [Adding a security profile on page 490](#) for relevant field descriptions.

The security profile is updated with your changes.

Procedure

Deleting security profiles

To delete an existing security profile:

- Step 1** Navigate to *Setup Tools > Security Profiles*.
 - Step 2** Select the security profile that you would like to delete.
 - Step 3** Click the **Delete** button.
-

The security profile is deleted.

Brand Management

The branding functionality enables providers to customize the System Administration Graphical User Interface (GUI) to their own colors, labels, icons, logo and general styling. The system is supplied with a default GUI that you are free to use. However, most providers will want to customize the front-end to be more appropriate to their own organization's "look and feel".

The term "Brand" describes a concept and an object. Branding includes all graphic elements of the system GUI. The elements making up a brand are contained in a ZIP file.

Note

The ZIP file format (*.ZIP) is a data compression and archive format. A ZIP file contains one or more files that have been compressed to reduce file size, or stored as-is. An application is required to "unzip" (access) a zip file and to create or "zip up" a ZIP file. A number of proprietary and open source compression applications exist such as WinAce®, WinRAR® and WinZip®. A number of mainstream operating systems now include built-in ZIP file support. This functionality is often referred to as *compressed folders*.

Brands can be added to your system in two ways, by importing a brand and by creating a new brand online using the brand editor. For more information on editing brands, see [Brand Editor Overview on page 496](#).

Procedure***Adding a Brand***

To add a brand:

- Step 1** Browse to *Setup Tools > Branding* .
 - Step 2** Click the **Add** button.
 - Step 3** Once you have made the required changes to the default brand in the Brand editor, enter a brand name in the brand name field and click the **Submit** button.
-

The brand will be added to the system and will be listed on the Brand Management page under the *Setup Tools* menu.

Procedure***Exporting a Brand***

To export a brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Click the **Export Brand** button adjacent to the brand that you would like to export.

- Step 3** Click the **Save As** button and specify a name and location for the brand (ZIP file). The brand will be exported and saved to the specified location.

Note

If you are exporting a brand to edit it, once you have finished making changes to the brand, use the Import function above to add your changes to the system. See: [Importing a Brand on page 495](#).

Procedure

Modifying a Brand

To modify a brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Select the *Name* (active text link) of the brand that you would like to modify.
- Step 3** Once you have made the required changes to the brand in the Brand editor, enter a brand name in the brand name field and click the **Submit** button. The brand will be updated in the system.

Procedure

Deleting a Brand
Note

- The system default brand cannot be deleted.
- On systems installed with the *cisco_hcs* brand, this brand cannot be deleted from the system and will be reverted to as system default brand when all other brands have been deleted from the system.

To delete a brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Click the **Delete** button adjacent to the brand that you would like to delete. Once you have confirmed the deletion operation, the brand will be deleted from the system.
-

Importing a Brand

Brands can be added to your system in two main manners, by importing a brand and by creating a new brand online using the brand editor.

Procedure

To import a brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Click the **Import Brand** button.
- Step 3** Click the **Browse** button and browse to the Brand file (ZIP file) that you would like to upload to the system.
- Step 4** Once you have selected the file you would like to upload, click the **Upload file** button.
-

Import a Brand Status

The Brand Upload Status page summarizes the state of a requested brand upload. When a brand is uploaded successfully, the user will receive a message stating that the brand was uploaded successfully. If the upload was not successful, the user will be presented with an error message that outlines the problem(s) encountered.

Brand Editor Overview

The online brand editor is launched via the **Add** button or by editing an existing brand.

Procedure

To access the brand manager by adding a new brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Click the **Add** button. The Brand editor will open.

Procedure

To access the brand manager by modifying a new brand:

- Step 1** Browse to *Setup Tools > Branding* .
- Step 2** Select the *Name* (active text link) of the brand that you would like to modify. The Brand editor will open.
-

Overview of the Brand Editing Tool

The brand editing tool screen consists of two key sections.

The upper section contains a preview of the brand that you are currently editing. The window contains a number of "placebo" or "dummy" elements that will assist you with visualizing your final brand.

The bottom section of the editing tool contains the *Editor* menu. This menu houses all of the controls needed for editing the brand.

Updating Elements

The base screen is divided into five core elements. These elements are configured by specifying the required changes and then dragging the changes to the specific element.

Procedure

To update an element within the brand editor:

- Step 1** Specify the modifications that you would like to make to the element. For example, specify a background color or background image. Colors can either be specified by entering their hex triplet (hexadecimal) values or they can be selected from the color pallet at the bottom of the page. You are able to change the color pallet by selecting the required pallet from the drop-down list. The standard options include *Common Colors* and *Grayscale*.

Note

- For aspects like backgrounds, only one variable can be specified, you cannot specify a background color and a background image for an element.

- The images that can be used as part of branding must first be uploaded to the system. To do this, browse to *Setup Tools > Images*, click the **Add** button and then **Browse** for image files before clicking the **Upload file** button.

Available controls include:

Control	Description
Image Name	Used to specify an image that you would like to add. Only images that have already been added to the system are available from this drop-down list. Selecting the Blank option will clear the current contents of this field.
Background Image	Used to specify a background image that you would like to use for one of the page elements. Only images that have already been added to the system are available from this drop-down list. Selecting the Blank option will clear the current contents of this field. Only one variable can be specified, you cannot specify a background color and a background image for an element.
Background Color	Used to specify a background color for one of the page elements, or for a button. When selecting a background color, first select the checkbox associated with the Background Color control. Colors are selected from the color pallet at the bottom of the page. You are able to change the color pallet by selecting the required pallet from the drop-down list. The standard options include Common Colors and Grayscale. Selecting the Blank option will clear the current contents of this field. Selecting the Default option will restore the default selection. Only one variable can be specified, you cannot specify a background color and a background image for an element.
Font Color	Used to specify the font colors for your brand, which would include normal text, links and the font color on buttons. When selecting a font color, first select the checkbox associated with the Font Color control. Colors are selected from the color pallet at the bottom of the page. You are able to change the color pallet by selecting the required pallet from the drop-down list. The standard options include Common Colors and Grayscale. Selecting the Blank option will clear the current contents of this field. Selecting the Default option will restore the default selection.
Text	Use this field to add custom text elements to a page element. Selecting the Blank option will clear the current contents of this field. Selecting the Default option will restore the default selection.
Brand Name	Use this field to specify the name of the brand. This name will be used when the brand is listed within the system and also for the ZIP file when it is exported.

Step 2

Once you have configured the changes that you would like to make to an element, you need to apply the changes in one of two ways:

- **Option 1:** Drag the "bull's eye" target to the section of the page that you would like to apply the changes to. Drag the bull's eye target by holding down your left mouse button while hovering over the target; while holding down the button, move your mouse over the element that you would like to modify and release your mouse button.
- **Option 2:** Select the **link** or **button** you would like to apply the changes to.

Step 3

Once you have made the required changes, click the **Submit** button. The brand will be updated and/or added to the system.

Note

- To undo changes you have made within the brand editor, click the **Clear All** button.
 - To make the brand that is currently being edited the system default, click the **Set as default system brand** button.
 - After making a brand the system default, the brand will not be applied until you logout then login to the system again.
-

Deploying Brands

Note

- Brands are deployed hierarchically.
 - A Brand is selected to be applied to an entity at any level in the hierarchy, e.g. Provider. In addition, brands are also assigned (made available) to the entity to be applied and assigned to further child level entities, and to administrators at the entities.
 - Only brands that are selected for the parent will be available for the child, for example, only if a brand is selected for the reseller is it available at the customer level.
 - Once the default is selected at a particular level, the default will roll down against all child entities, making it the default for all the child level entities. However, if other brands have been assigned or made available as optional brands to a child, then it is possible to assign an administrator at the child level to one of those other optional brands, instead of keeping the inherited default brand. These other optional brands are also available to be assigned to the next level entities in the hierarchy.
-

Provider

Manage Defaults and Available Brands

Procedure

Follow these steps:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the relevant *Provider* (active link).
- Step 3** Select the relevant brand to be applied as the Provider's default brand.

Select the brands that will be:

- Applied to the Provider's administrators
- Available from the provider for applying and assigning to any of its Resellers and their administrators

- Step 4** Click the **Modify** button to save the brand selections you have made.
-

Reseller

Manage Defaults and Available Brands

Procedure

Follow these steps:

- Step 1** Browse to *General Administration > Resellers*.
 - Step 2** Select the relevant *Reseller* (active text link).
 - Step 3** Select the relevant brand to be applied as the Reseller's default brand.
Select the brands that will be:
 - Applied to the Reseller's administrators.
 - Available from the Reseller for applying and assigning to any of its Customers and their administrators.
 - Step 4** Click the **Modify** button to save the brand selections you have made.
-

Customer

Manage defaults and available brands

Procedure

Follow these steps:

- Step 1** Browse to *General Administration > Customers*.
 - Step 2** Select the relevant *Customer* (active link).
 - Step 3** Select the relevant brand to be applied as the Customer's default brand.
Select the brands that will be:
 - Applied to the Customer's administrators
 - Available from the Customer for applying and assigning to any of its Divisions and their administrators
 - Step 4** Click the **Modify** button to save the brand selections you have made.
-

Division

Manage Defaults and Available Brands

Procedure

Follow these steps:

- Step 1** Browse to *General Administration > Division*.
- Step 2** Select the relevant *Division* (active link).
- Step 3** Select the relevant brand to be applied as the Division's default brand.
Select the brands that will be:
 - Applied to the Division's administrators.

- Available from the Division for applying and assigning to any of its Locations and their administrators.

Step 4 Click the **Modify** button to save the brand selections you have made.

Location

Manage Defaults and Available Brands

Procedure

Follow these steps:

- Step 1** Browse to *General Administration > Location*.
- Step 2** Select the relevant *Location* (active link).
- Step 3** Select the relevant brand to be applied as the Location's default brand.
- Step 4** Select the brands that will be available for Location's administrator accounts.
- Step 5** Click the **Modify** button to save the brand selections you have made.
-

Administrators

Procedure

To apply a brand to an Administrator at any of the levels in the hierarchy (Provider, Reseller, Customer, Division or Location):

- Step 1** Browse to *General Administration > Administration Users*.
- Step 2** Select the relevant *Username* (active text link).
- Step 3** Select the relevant brand to be applied to the user's profile.
- Step 4** Click the **Modify** button to save the brand selection you have made.
-

Feature Group Administration

This section covers Feature Group Management and the features that are available when adding or modifying a Feature Group.

Feature Group Management

Feature Groups help to customize the services offered by a Provider to its Customers, and assigned by Customer or location admin to its End users and phones. They define a set of services, including Class of Service (CoS) to be allocated to an end user or a Phone. You cannot authorize Services for end users and phones any other way. Understanding Feature Groups and refining their use can significantly improve the perception of the IPT systems by its Users. Poor Feature Group definition will result in a poor service definition to users and phones.

Note

- Feature Groups determine the set of services available for a phone when registered and a user when created.
- Feature Groups are allocated and managed at the Customer level and are common across all Locations within that Customer. At least one feature group

must be available for the customer in order to register phones and create end users.

- Feature Groups are generally defined and created according to service packages offered by the Services Provider. Normally, the Provider will want to control the Customers Feature Groups as this may affect the set of services purchased by that specific customer. For example: the number of lines/DDIs allowed is defined in the Feature Group. If the customer agreement with the provider is for 1DDI per phone only, definition of Feature Group allows the customer to affect this. Or the use of Billing codes related CoS - again a service that the Service Provider may want to charge for.
- Although feature groups can be created at customer level we recommend that you create Feature Templates at the provider level and only allocate them to the customer as applicable. This allows for better control and management of the services packages offered by the provider.

[Adding a Feature Group on page 503](#)

Feature groups can be added or created from a pre-defined a feature group template. The feature group templates are created and managed at provider level (see [Feature Group Template Management on page 677](#)). Once created, the feature group template can be modified for the customer as required.

Note

Once a feature group is created from a template for the customer, it is managed at this level only. Changes to the template that it originated from will not affect the feature group.

Procedure

Create from Template

- Step 1** Click the **Create from Template** button on the *Feature Group Management* screen. This opens the *Feature Group Template Selection* screen with the list of the provider feature templates available to copy from.

The following information is available in this list:

Field	Description	Remarks
Create from Template	Button allowing you to create a feature group from the named feature group template	Button
Name	Name of the feature group template	-
Description	Feature group template description	-
New Name	The name for the feature group at the customer level once created from the feature group template.	This is a mandatory field.

- Step 2** Enter a new name next to the feature group template that you wish to create a copy from and click the **Create From Template** button next to it. A new feature group for the customer is created with the services as defined in the selected feature group template.

Note

Once created at the customer level, the feature group is available for use or update as required.

Procedure

Bulk Updating Feature Groups

This feature allows you to bulk update feature group settings for several feature groups at the same time. Firstly select the feature groups to update, and then update the settings that you want to update for the selected feature groups.

To update the settings for several feature groups at the same time:

- Step 1** Browse to *General Administration > Feature Groups*. The *Feature Group Management* screen is displayed.
- Step 2** Click the **Bulk Update** button. The *Bulk Feature Group Update* screen is displayed.
- Step 3** Select the *Update* checkboxes adjacent to each of the feature groups that you want to update.
- Step 4** Click the **Submit** button.
- Step 5** Confirm that all the feature groups that you want to update are listed under the section *Feature Groups to Update*.
- Step 6** Select the relevant left-most checkboxes adjacent to all the features that you want to update, then configure the *Activated* setting (text box, drop-down or checkbox) to apply the change to the selected features. For more details about the various feature settings refer to [Features Available when Adding or Modifying a Feature Group on page 505](#).

Note

If you select the left-most checkbox in the *Common Line settings (Call Forward)* section, all the respective settings are applied, namely *Destination*, *ForwardToVoicemail*, *Cos Editable*, and *CoS* (selection).

- Step 7** Click the **Submit** button when complete to update the selected feature settings for all the selected feature groups.

Procedure

Modify Feature Groups

To modify the settings of a feature group:

- Step 1** Navigate, at the customer level, to the *General Administration* screen.
- Step 2** Select the required customer, by selecting the customer *Name* (active text link).
- Step 3** Once you have selected the required customer, select the *Feature Groups* tab, under the *General Administration* menu.
- Step 4** Select the feature group that you would like to modify, by selecting the feature group *Name* (active text link).
- Step 5** Make the required changes to the feature group, and then click the **Modify** button.

For the attributes that are available on the *Manage Feature Group* screen, see: [Features Available when Adding or Modifying a Feature Group on page 505](#).

Procedure

Delete Feature Groups

To delete a feature group:

-
- Step 1** Navigate, at the customer level, to the *General Administration* screen.
 - Step 2** Select the required customer, by selecting the *Customer Name* active text link.
 - Step 3** Once you have selected the required customer select the *Feature Groups* tab, under the *General Administration* menu.
 - Step 4** Select the feature group that you would like to delete, by selecting the relevant feature group *Name* (active text link).
 - Step 5** Click the **Delete** button. After confirming the deletion, the feature group is removed from the system.
-

Disabling Features that are in Use

Certain services within the feature group cannot be removed while users assigned to the feature group are using the services. Before disabling these services, make sure that no users are currently using the affected services. Services affected by this validation include Single Number Reach, User Mobility, Voicemail and Extension Mobility Cross Cluster. A number of settings within feature groups are not governed by the feature group validation policy outlined above. The work flow of how the modification of feature groups is handled by the system is outlined below.

If the modification to the feature group removes services (for instance Single Number Reach, User Mobility, Voicemail and Extension Mobility Cross Cluster) the services are not removed from the user, however, the services are no longer accessible for the user (the setup services cannot be managed or deleted).

If a feature is disabled in the feature group, this does not take effect immediately on the users. The setting is removed from the phone management and roaming (mobility) profile screen, however, the setting is still configured on the Unified CM until a Modification of the profile/phone is done (or the OPs tools - *Refresh All Phones Feature at a location*).

If the modification to the feature group enables services within the feature group, they are available to the user for configuration.

If the modification to the feature group adds new settings to the feature group, they are available to be configured for the user (but no changes are made to the existing user configuration in the Unified CM.)

Procedure

Disabling of SNR when in use:

Disabling the SNR feature within a Feature Group does not disable a provisioned SNR feature for an End User, but may impact the usability of the provisioned SNR feature.

- To re-sync supported features per Location, it is required to perform the OpsTool - Re-apply feature group capabilities for a given location for each affected Location, once the Feature Group has been updated.
-

A message is displayed warning the user and giving them the option to abort the operation, but if the user chooses to proceed, the transaction will not fail.

Adding a Feature Group

Procedure

To add a feature group:

- Step 1** Navigate, at the Customer level, to the *General Administration* screen.

- Step 2** Select the required customer, by selecting the customer *Name* (active text link).
 - Step 3** Once you have selected the required customer select the *Feature Groups* menu option under *General Administration*.
 - Step 4** Click the **Add** button on the *Feature Group Management* screen. The *Add Feature Group* screen is displayed.
 - Step 5** Enter the required information in the relevant fields. For the features/fields and descriptions that are available see [Features Available when Adding or Modifying a Feature Group on page 505](#).
-

Manage Feature Group

Procedure

Modify Feature Groups

To modify the settings of a feature group (at the customer level):

- Step 1** Browse to *General Administration > Feature Groups*.
 - Step 2** Select the feature group *Name* (active text link) that you would like to modify.
 - Step 3** Make the required changes to the feature group. For the features/fields and descriptions that are available see [Features Available when Adding or Modifying a Feature Group on page 505](#).
 - Step 4** Click the **Modify** button located at the bottom-left of the screen when complete.
-

Disabling Features that are in Use

Certain services within the feature group cannot be removed while users assigned to the feature group are using the services. Before disabling these services, make sure that no users are currently using the affected services. Services affected by this validation include Single Number Reach, User Mobility, Voicemail and Extension Mobility Cross Cluster. A number of settings within feature groups are not governed by the feature group validation policy outlined above. The work flow of how the modification of feature groups is handled by the system is outlined below.

If the modification to the feature group removes services (for instance Single Number Reach, User Mobility, Voicemail and Extension Mobility Cross Cluster) the services are not removed from the user, however, the services are no longer accessible for the user (the setup services cannot be managed or deleted)

If a feature is disabled in the feature group, this does not take affect immediately on the users. The setting is removed from the phone management and roaming (mobility) profile screen, however, the setting is still configured on the Unified CM until a Modification of the profile/phone is done (or the Ops tools - *Refresh All Phones Feature at a location*).

If the modification to the feature group eases services with the feature group, this makes them available to the user to be configured.

If the modification to the feature group adds new settings to the feature group, they are available to be configured for the user (but no changes are made to the existing user configuration in the Unified CM.)

Procedure

Delete Feature Groups

To delete a feature group (at the customer level):

- Step 1** Browse to *General Administration > Feature Groups*.
- Step 2** Select the feature group *Name* (active text link) that you would like to delete.

- Step 3** Click the **Delete** button located at the bottom-right of the screen. After confirming the deletion, the feature group is removed from the system.

Features Available when Adding or Modifying a Feature Group

The following fields, options and features are available when adding or modifying a Feature Group/Feature Group Template (see below):

Details	
Name	The name of the feature group/feature group template.
Description	A short description of the feature group/feature group template you are modifying.
Outbound calls limitations	<p>The CSS is set appropriately on the lines associated with the phone or extension mobility profile (if applicable). Select the required outbound calls limitations from the drop-down list, default = Internal only voice calls.</p> <p>Note</p> <ul style="list-style-type: none"> As soon as a phone line is registered with the default <i>Line Class of Service</i> (that is the <i>Outbound calls limitations</i> value selected here), this value is applied to the line and remains the COS value for that line, even when the Feature Group value for Outbound calls limitations is modified. When selecting a COS, the corresponding CSS must exist on Unified CM.
Call forward limitations	The Call Forward CSS's are set appropriately on the lines associated with the phone or extension mobility profile (if applicable). Select the required call forward limitations from the drop-down list, default = Default Limitations.
Voicemail Template	This setting does not apply for Cisco HCS.
Inbound call options	<p>Controls the maximum number of DDI lines that could be registered/defined on the phone/extension mobility profile. For example, if the value is set to two, the phone could be registered with one line, but no more than two.</p> <p>If none is allowed, a phone/extension mobility profile can only be registered/defined with an internal extension number.</p> <p>Select the required option from the drop-down list, default = Don't allow Direct Dial Inwards calls.</p>
Number of extensions or lines	Controls the maximum number of Extension lines (DDI or non DDI) that could be registered/defined on the phone/extension mobility profile. For example, if the value is set to two, the phone could be registered with one line, but no more than two. Select the required option from the drop-down list, default = One number - DDI or Extension.
Idle URL	Allows selection of a URL for an image or an application to execute when a phone has been idle for a specified period of time. Service of type idleurl must be configured first. Default = None.

Note

Click the **Check All** or **Uncheck All** button to select/unselect **all** features simultaneously if required. This can be done in the *Details* section of the screen

to select/unselect **all** features on the screen, or in each specific section, for example *Value Add*, *Common Line Settings (Line Feature, etc.)* of the screen to select/unselect the features relevant to that particular section **only**.

Value Add These are additional services/features that can be enabled for the user. Enable or disable the value added features by selecting or unselecting the relevant checkbox/es. For more details, see also: <ul style="list-style-type: none"> • Conference Service Management on page 626 • Mobile Connect/Single Number Reach (SNR) on page 417 • UC Central on page 874 • the section on Single Number Reach in the Self-Care Guide • Manage Voicemail Accounts on page 867 	
Conferencing	<p>When a phone is registered, or a user is created within a feature group containing this service feature enabled, conference accounts can be created for a conference service, e.g. Webex. Once conferencing has been activated within the users feature group, administrators can enable and configure the user's conference account settings via the <i>Location Administration > End Users</i> menu. Default = Not selected.</p> <p>Note: This checkbox must be selected in order to provision the Webex conference feature for the user.</p>
Extension Mobility Cross Cluster	<p>If this setting is enabled, the existing extension mobility feature within a single cluster, is extended to function across multiple Cisco Unified Communications Manager (Unified CM) clusters. This means that if phone A is on cluster 1 and phone B is on cluster 2, a user can login to either phone, and their phone service operate using the same phone profile.</p> <p>Note</p> <p>To enable the <i>Extension Mobility Cross Cluster</i> feature, the <i>Extension Mobility Cross Cluster</i>, <i>User mobility</i>, and <i>Allow user login to phone</i> checkboxes must be enabled (selected), and the <i>BVSMUserRoaming</i> option on the <i>Provider Administration > Providers > Preferences and Settings</i> screen must be disabled (not selected).</p> <p>If the <i>BVSMUserRoaming</i> option is enabled, then only normal Extension Mobility capability is available irrespective of the <i>Extension Mobility Cross Cluster</i> setting.</p>
IP Phone Services Management	<p>If this setting is enabled, administrators can manage the phone services for end users' devices and extension mobility profiles. Default = Not selected.</p>
Presence	<p>Enables the use of Cisco Unified Presence (Unified Presence). Once Unified Presence has been activated within the users feature group, administrators can enable and configure the user's Unified Presence settings via the <i>Location Administration > End Users</i> menu. Default = Not selected.</p>
Single Number Reach / Mobile Connect capabilities	<p>This setting is used to determine whether a user has access to the Single Number Reach functionality. Default = Not selected.</p>

UC Central	If this setting is enabled, an administrator of the end user can manage the user's UC Central client configuration. The administrator is specifically able to select an extension to be used for connecting to UC Central. Default = Not selected.
Voicemail	<p>Controls whether a Voicemail account can be created for a specific user. If this feature is included in the Feature Group associated with the User, an administrator can create a voicemail box for the user.</p> <p>Note</p> <p>No configuration occurs; this setting assumes that all pre-requisite for provisioning Voicemail have been met. Default = Not selected.</p>
<p>Common Line settings (Line Feature) - these are line settings that affect all appearances of the line on all devices. Enable or disable the line features by selecting or unselecting the relevant checkbox.</p> <p>For more information, see also: Managing the Phone on page 806.</p>	
Alerting Name	<p>If this option is selected, administrators can manage a phone's / user's extension mobility profile alerting name. Default = Not selected.</p> <p>Note</p> <p>There is no default Alerting Name, if the Alerting Name option is enabled in the Feature Group, and the Alerting Name is left blank, the value in Cisco Unified Communications Manager will also be blank.</p>
Alerting Name ASCII	If this option is selected, administrators can manage a phone's/ user's extension mobility profile ASCII value for Alerting Names.
Auto answer	If this setting is enabled on the line, the line auto answers if a call arrives on the line. Default = Not selected.
Call forward calling search space activation policy	Enables Call Forward calling search space activation policy to enable the administrator to set the Call Forward calling search space activation policy settings of a phone/user's mobility profile. For more information on these settings, refer to the relevant Unified CM documentation. Default = Not selected.
Cloned line	If this setting is enabled, Cloned Line functionality is enabled and an administrator of the phone can manage the Cloned Line settings. Default = Not selected.
Contact Center Agent Line	This setting is used to enable the provisioning of the line as a contact center line. This results in the line receiving a modified line description field. If this setting is enabled on the line, then the description is changed to start with the value defined in the global setting CCLinePrefix. The rest of the description remains the same. For example 'CC_Line Line 55555555 for a phone'. Default = Not selected.
Hold reversion notification interval	When enabled, the Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. This setting enables administrators to configure the duration between warnings. Default = Not selected.
Hold reversion ring duration	When enabled, the Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. This setting enables administrators to configure the duration. Default = Not selected.
Hot line	If this setting is enabled, an administrator of the phone can define the destination for a call initiated if the line is selected. (This is the standard PLAR feature). Default = Not selected.

Line Class of Service	If this option is enabled, administrators can select the relevant line class of Service. Default = Not selected.
Music on hold	Enables the administrator of the phone to define a per line MoH track. Default = Not selected.
No answer ring duration	If this setting is enabled, an administrator of the phone / extension mobility profile can set a value for this setting. Value is in seconds and the range is from zero to the value of the Max. No Answer Ring Duration parameter for the phone type (7960 for Mobility). Default = Not selected.
Private Line settings (Phone Line Feature) - these are settings that are unique per line instance (line/device combination). Enable or disable the phone line features by selecting or unselecting the relevant checkbox. For more information, see also: Managing the Phone on page 806 .	
Call waiting busy trigger	Enables Call Waiting and enables the administrator to manage the Call Waiting settings. Default = Not selected.
Display name (Caller Line ID)	Controls whether the Display Name of a line on a phone / extension mobility profile can be managed. Default = Not selected.
Display name ASCII	Controls whether the ASCII value for a Display Name of a line on a phone/ extension mobility profile can be managed.
Forwarded Call Display - Caller Name	This line feature allows a receiver of forwarded calls to display the name of the call originator. When a line is first registered, this has a default value of 'True'. Selected = feature available; Not selected = feature not visible.
Forwarded Call Display - Caller Number	This line feature allows a receiver of forwarded calls to display the number of the call originator. When a line is first registered, this has a default value of 'False'. Selected = feature available; Not selected = feature not visible.
Forwarded Call Display - Dialed Number	This line feature allows a receiver of forwarded calls to display the line number that the originator attempted to reach. When a line is first registered, this has a default value of 'True'. Selected = feature available; Not selected = feature not visible.
Forwarded Call Display - Redirected Number	This line feature allows a receiver of forwarded calls to display the number that was redirected. When a line is first registered, this has a default value of 'False'. Selected = feature available; Not selected = feature not visible.
Hide Line from Corporate Directory	An administrator can hide (select checkbox) an end user's shared line from displaying in the corporate directory. Default = Not selected.
Label	Controls whether the Line Label on a line on a phone can be managed. Default = Not selected.
Label ASCII	Controls whether the ASCII value for a Line Label on a line on a phone can be managed. Default = Not selected.
Line mask	Controls whether the Line Mask on a phone / extension mobility Profile can be managed. Default = Not selected.
Max calls waiting	The maximum number of calls that can be queued for waiting. Once this number is reached, the next caller gets a busy tone. Default = Not selected.

Message waiting lamp policy	If this setting is enabled, an administrator of the phone / extension mobility profile is can set a value for this setting. Selected from <i>Use System Policy, Light and Prompt, Prompt Only, Light Only</i> and <i>None</i> . Default = Not selected.
Recording Option	>If this setting is enabled, an administrator of the phone / extension mobility profile can set a value for this setting. Selected from <i>Call Recording Disabled, Automatic Call Recording Enabled</i> and <i>Selective Call Recording Enabled</i> . Default = Not selected.
Recording Profile	If this setting is enabled, an administrator of the phone / extension mobility profile can configure a recording profile. Default = Not selected.
Ring setting - Phone active	If this setting is enabled, an administrator of the phone / extension mobility profile can set a value for this setting. Select from <i>Use System Policy, Disable, Flash Only, Ring Once, Ring</i> and <i>Beep Only</i> . Default = Not selected.
Ring setting - Phone idle	If this setting is enabled, an administrator of the phone / extension mobility profile can set a value for this setting. Select from <i>Use System Policy, Disable, Flash Only, Ring Once, Ring</i> and <i>Beep Only</i> . Default = Not selected.
Handset - These are settings that affect the base device operation. Enable or disable the handset features by selecting or unselecting the relevant checkbox.	
Advanced Phone Settings	If this setting is enabled, an administrator of the phone can set a phone's imported advanced settings. Default = Not selected.
Allow user login to phone	Controls whether the Login service is available on the phone. This is achieved by subscribing the phone to the roaming Login / Logout service. Default = Not selected.
Built-in Bridge	When this feature is selected an administrator can manage the Built-in Bridge setting for a phone. Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list on the Phone Management screen (select <i>On, Off, or Default</i>).
Busy lamp fields	If this setting is enabled, an administrator of the phone / extension mobility profile can manage the busy lamp fields. Default = Not selected.
Cache username on phone	If this feature is enabled, the system caches the username of the last user that was logged into the phone. Default = Not selected.
Corporate phone book	Determines if the <i>Corporate Directory</i> menu option is available in Self Care. Default = Selected.
Fax	This only affects analog ports. If this setting is enabled, the analog port being defined is placed in the Fax Device Pool on the Cisco Unified Communications Manager (Unified CM). Default = Not selected.
Personal phone book	Determines if the <i>Personal Directory</i> menu option is available in Self Care. Default = Selected.
Privacy	When this feature is selected an administrator can manage the privacy settings for a phone, SNR and Mobility line. When privacy is enabled on the Phone Management screen, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls.
SRST	Allows administrators to enable SRST for the specified phone which places the phone in the SRST device pool. Default = Not selected.

Service URLs	Controls whether Service URLs on a phone / extension mobility profile can be managed. Default = Not selected.
Speed dials	Controls whether the Speed Dials on a phone / extension mobility profile can be managed. Default = Not selected.
User - enable or disable the following user features by selecting or unselecting the relevant checkbox	
User extension mobility	Controls whether an extension mobility profile can be created for the user. If this feature is included in the Feature Group associated with a User, an administrator can create an extension mobility profile for the user. Default = Not selected.
<p>Voicemail Settings - These are additional groups of settings that can be defined on the voicemail box. Enable or disable the voicemail settings features by selecting or unselecting the relevant checkbox.</p> <p>Note</p> <p>The features below only function if the <i>Voicemail</i> checkbox has been selected (see under Value Add section above).</p>	
Alternate Extension	The status of this checkbox determines if alternate extensions are available to subscribers of the Voicemail service in the selected feature group. Default = Not selected (disabled).
Caller Input	The status of this checkbox determines if the caller input feature are available to the subscribers of the Voicemail service in the selected feature group. Default = Not selected (disabled).
Notification Device	The status of this checkbox determines if the notification device feature [SMS, Phone, Email (SMTP) or Pager] is available to subscribers of the Voicemail service in the selected feature group. Default = Not selected (disabled).
Visual Voicemail	The status of this checkbox determines if visual voicemail feature is available to subscribers of the Voicemail service in the selected feature group. Default = Not selected (disabled).

<p>Common Line settings (Call Forward) - These are call forward settings that can be defined on the device.</p> <p>The following checkboxes/drop-down lists are available for each call forward setting (as shown below):</p> <ul style="list-style-type: none"> • Destination (checkbox) - select this checkbox to expose the call forward destination setting on the phone/extension mobility profile management screen in CUCDM and Self Care. • ForwardToVoicemail (checkbox) - select this checkbox to expose the call forward to voicemail checkbox on the phone/extension mobility profile management screen in CUCDM and Self Care. • CoS Editable (checkbox) - select this checkbox to make the CoS field editable on the phone/extension mobility profile management screen in CUCDM and Self Care. • CoS (drop-down) - allows you to set the default CoS for the specified call forward setting. Default setting = <i>Use Feature Group Default</i>, which inherits the CoS value from the Call Forward Limitations field (see <i>Details / Call forward limitations</i> field above). The <i>None</i> option sets the Unified CM CSS value to <i>None</i>. <p>Note</p> <p>Certain call forward settings, that is <i>Forward Busy</i>, <i>Forward No Answer</i>, <i>Forward No Coverage</i> and <i>Forward Unregistered</i>, can be configured in a combined manner (including external and internal) as a 'group' or separately (external or internal). The 'combined' and 'separate' checkboxes cannot be selected at the same time. For example, if you select (enable) the <i>Forward Busy (Activated or ForwardToVoicemail)</i> checkbox, the <i>Forward Busy External</i> and <i>Forward Busy Internal</i> checkboxes are not available, and visa-versa if you select any of the <i>Forward Busy External</i> or <i>Forward Busy Internal</i> checkboxes.</p>	
Forward All	<p>The settings in this row specify the forwarding treatment for all calls to this directory number.</p> <p>Note</p> <ul style="list-style-type: none"> • This setting takes precedence over all other call forward settings. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i>. • If this checkbox is selected, the <i>Forward All Secondary CoS</i> field is exposed in the <i>Common line settings (Call Forward)</i> section of the associated <i>Phone Managment</i> screen.
Forward All Secondary CoS	<p>Because call forwarding is a line-based feature, in cases where the device calling search space is unknown, CUCDM uses only the line calling search space to forward the call. If the line calling search space is restrictive and not routable, the forward attempt fails. This field provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Checkbox default = not selected (disabled) and drop-down default = <i>None</i>.</p>
Forward Busy	<p>The settings in this row specify the forwarding treatment for calls if the directory number is busy. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i>.</p>

Forward Busy External	The settings in this row specify the forwarding treatment for external calls if the directory number is busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward Busy Internal	The settings in this row specify the forwarding treatment for internal calls if the directory number is busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Answer	The settings in this row specify the forwarding treatment for calls if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Answer External	The settings in this row specify the forwarding treatment for external calls if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Answer Internal	The settings in this row specify the forwarding treatment for internal calls if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Coverage	The settings in this row specify the forwarding treatment for calls when there is a faulty connection between Unified CM and the device. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Coverage External	The settings in this row specify the forwarding treatment for external calls when there is a faulty connection between Unified CM and the device. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward No Coverage Internal	The settings in this row specify the forwarding treatment for internal calls when there is a faulty connection between Unified CM and the device. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward Unregistered	The settings in this row specify the forwarding treatment for unregistered directory number (DN) calls. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward Unregistered External	The settings in this row specify the forwarding treatment for unregistered external directory number (DN) calls. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward Unregistered Internal	The settings in this row specify the forwarding treatment for unregistered internal directory number (DN) calls. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .
Forward on CTI Failure	This field applies only to CTI route points and CTI ports. The settings in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Checkboxes default = not selected (disabled) and drop-down default = <i>Use Feature Group Default</i> .

Device Group Management

Device Groups are an optional administrative sub-division of Locations. They are used for defining a set of resources within a Location. These do not have any impact on the Cisco Unified Communications Manager for the Location.

- Renaming Device Groups

The name used within the system for Device Groups may be changed to something else to suit the customers needs. A common title for Device Groups is "Tenants". This change is a system level setting and affects the entire installation. To change the name, navigate to *Setup Tools > Global Setting* and select the *DeviceGroupName* function.

Two sets of boxes are displayed. The first set is for the singular *Device Group* and the second for the plural *Device Groups*. For each of these a word or phrase may be configured for each language used by the installation.

Once changed, the new names are used for the buttons, menu items, headings and labels within the system.

- Enabling Device Groups

Device Groups may be enabled or disabled for each Provider within the system. To enable Device Groups, navigate to *Provider Administration > Providers > Provider Name* and click the **Preferences** button. Select *DeviceGroupsSupported* and then select the checkbox to enable the setting. To disable the setting clear the checkbox. Click the **Modify** button when complete.

Disabling Device Groups does not remove any Device Groups already configured, or affect their resources. It only disables their functionality and visibility.

Procedure

Adding a Device Group

To add a device group:

- Step 1** Browse to *General Administration > Device Groups*.

Notes:

- If this option is not available, please contact your provider to ensure that this feature is enabled.
- Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

- Step 2** Click the **Add** button.

- Step 3** Enter a name (mandatory field) and description (optional) for the device group then click the **Add** button.

The device group is added to the system.

Procedure

Modifying a Device Groups Details

To modify a device group:

- Step 1** Browse to *General Administration > Device Groups*.

Note

- If this option is not available, please contact your provider to ensure that this feature is enabled.
- Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

Step 2 Select the *Name* (active text link) of the device group that you would like to modify.

Step 3 Modify the required fields then click the *Modify* button.

The profile is updated with the modifications.

Procedure

Modifying a Device Groups Counts

To modify a device group:

Step 1 Browse to *General Administration > Device Groups*.

Note

- If this option is not available, please contact your provider to ensure that this feature is enabled.
- Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

Step 2 Select the *Name* (active text link) of the device group that you would like to modify.

Step 3 Select the required resource, for example *Number of phones* (active text link) from the *Counts* section of the screen.

Step 4 To assign resources, select the required resources in the *Available* area, and then click the *Assign* button to move them to the *Assigned* area.

or

To remove resources, select the relevant resources in the *Assigned* area, and then click the **Remove** button to move them back to the *Available* area.

Note

To assign multiple resources at once, use the *Ctrl* or *Shift* key to make multiple selections in the list.

Step 5 Click the **Update** button when complete.

The profile is updated with the modifications.

Procedure

Deleting a Device Group

To delete a Device Group:

Step 1 Browse to *General Administration > Device Groups*.

Notes:

- If this option is not available, please contact your provider to ensure that this feature is enabled.
- Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

Step 2 Select the *Name* (active text link) of the device group that you would like to delete.

Step 3 Click the **Delete** button.

After confirmation, the device group is deleted from the system.

Operations Tools

Operations Tools allow for the automation of multi-step processes, such as de-registering all phones in a location. The operations tools are not normally used in day to day operations.

The operations tools are typically used for testing purposes, when a 360 degree test needs to be performed, such as adding a location, deleting a location and then adding the same location again. They are also very useful for refreshing a location when adding a new dial plan to legacy locations.

Operation tools were initially created for super users and the internal testing group, however, many customers were also keen to have access to these tools. As a result, the operations tools are now available to Provider Administrators.

Procedure

Running Operation Tools

To run an operation tool:

Step 1 Browse to the *Operations Tools* page under *General Tools* menu.

Note

If you cannot find the tool you are looking for, select the **Next** button, this will take you to a second page of tools.

Step 2 To run one of the tools, select the relevant active text name.

Certain tools will present you with a confirmation page before proceeding while other tools will execute immediately.

Note: While running operations tools, you can perform other tasks within the system.

For the available tools, see: [Operations Tools on page 950](#)

Transaction Log and Search Report

The system's transaction management screen enables administrators on all levels to search for transactions executed by any user within their own domain.

Using the transaction search screen

In the system, browse to *General Tools > Transactions*.

The following new search types are available to all administrators:

- All Transactions
- Action
- My Transactions
- Selected User
- Failed Transactions
- In Progress
- Not Processed
- Succeeded
- After Transaction
- Before Transaction
- Cancelled

Two exclude filters have been provided:

- **Exclude BVSMWeb transactions:** This will exclude all transactions executed by the admin Web user (i.e. transactions executed from a phone) from the search results.
- **Exclude end user transactions:** This will exclude all transactions executed by end users (level 6) from the search results.

Access to Transaction Logs for End Users

End users do not have access to the transaction search feature in the system. End users can view their own transactions in Self Care.

In Self Care, log in as an end user and select the *My Transactions* link to view transactions.

The search feature behaves differently depending on what value the user searches on.

When a user enters a number in the search field, the system would return a transaction with Transaction Key that matches the search phrase exactly.

When a user enters text in the search field, the system would return all transactions that contain the search phrase in the transactions action.

Bulk Administration

Bulk administration makes it easy for administrators to carry out transactions on items in bulk. Items are searched for and selected on the GUI, listed explicitly in valid MS Excel .xls input files, or specified by a combination of these methods.

Input files can be exported from search results and can be modified further, or created manually. The transactions that are available for a selected item type depends on the item type. The available item types are shown on the *Select item* drop-down list at the top of the main screen. All the items of a type have unique identifiers in the system. Examples of item types are *Device/Phone*¹ and *End User*.

¹These refer to the same item type, but are identified by device name and MAC address respectively.

To access the Bulk administration functionality from the GUI menu, select *General Tools > Bulk Administration*.

The Bulk administration screen is divided into groups of controls that allow for types of tasks available for the selected item type. The full list of tasks that may be available from the main screen are:

- Search

The **Search** button is selected to carry out this task. For a selected item type from the *Select item* drop-down list, a number of search options are available:

- The *Quick Search* group of controls is used to specify the search parameters for a selected item type. The search is done by selecting the *Quick Search* radio button. The *Select Target* drop-down list displays available hierarchy entries for the item type.

For some selected item types, additional parameters can be added (or removed) and show as 3-column rows of drop-down controls below the *Select Target* drop-down list:

- The first column lists properties of the selected item type. A property is selected to specify the additional search parameter. Constraints and constraint values to be applied to this property are added in the second and third columns of the parameter row.

A logical OR can be added to a search by selecting *~OR~* from the first column of the drop-down row. The logical OR applies between the groups of rows that are separated by the *~OR~* row.

- The second column drop-down list shows the available parameter search constraints to be applied to the value entered in the third column input box. For a search parameter, the selected property can then for example start with (*Starts with*) or contain (*Contains*) the value that is entered in the third column input box.
- The third column is an input box to be used to specify the values to apply to the search parameter and is used in conjunction with the selected property in the first column and the constraint in the second column.

The *add del* links next to a parameter row is used to add or remove parameter rows.

When the **Search** button is clicked, the results are shown on the preview screen - see [Bulk Administration Preview and Add on page 518](#).

- The *Upload item identity file* group of controls allows for a "file-as-search" method whereby the list of items to be searched for is uploaded as a specially formatted MS Excel *.xls* file. The file is called an *identity* file since it contains columns to uniquely identify the items in the rows of the spreadsheet. For more details on the input file format, see: [Bulk Administration file formats on page 520](#).

This file format can be created on the preview screen that displays the search results by using the **Get Excel Identity file** button - see [Bulk Administration Preview and Add on page 518](#). The created file can serve as a formatted template to be refined and modified as required.

Note

The search results displayed when using an uploaded, unmodified input file of items are the same as the displayed result list of items of the search on the preview screen that was used to create the input file.

- A combination of Quick Search and an uploaded identity file. Select the *Combine* checkbox to combine Quick Search parameters with items in a MS Excel Identity file.
- Add

Note

The **Add** button will only be available on this screen for those item types that can be added.

The **Add** button is selected to carry out this task on the preview screen - see [Bulk Administration Preview and Add on page 518](#).

- Execute a file

An action is carried out on an input file or the action is to export a raw API file. In accordance with the selected item from the *Select item* drop-down list, the *Action:* drop-down list in this group shows available actions that can be carried out.

Note

For an input file, the selected action will be carried out on item rows in the file *below the action with the same name in the input file*. In this way, only a selected action in an input file is carried out on the items below it.

The *Use file defined* option in this list will carry out all the actions in sequence as they are specified in the input file. For more details on the input file, see: [Bulk Administration file formats on page 520](#).

The drop-down list next to the **Execute** button has three options:

- *Execute immediately*: the transaction will immediately be added to the transaction queue when the **Execute** button is clicked.
- *Schedule*: the transaction will be scheduled for execution at the date and time as entered in the *Scheduled Date* and *Time* input boxes.
- *Export*: a `.xls` file is created in raw API format when the **Execute** button is clicked - see: [Bulk Administration file formats on page 520](#). No transaction is carried out.

Bulk Administration Preview and Add

If the **Search** or **Add** button is selected on the *Bulk Administration* screen, a search results screen is displayed (based on the search criteria entered) or an Add screen (for the relevant item selected) is displayed respectively (see below)

From these screens, a *Return to Bulk Administration* link is available to return to the main screen.

Search results

Search results are shown in the *Preview items and select further action* list frame of the preview screen.

The heading of the list hows:

- The type of search that was carried out (*List source:*)
- The selected item type (*Item type:*)
- *Search Details* that show the selected *Hierarchy* and all parameters as a *Filter*.

The body of the result list shows a checkbox next to each result. By default, all result checkboxes are selected. Items on the list can be selected and de-selected as required for a transaction or file input. Many results are grouped on pages to the selected *Items per page* value below the list frame.

The *Select Transaction and Input Method* group of controls are used to specify the task to carry out on the selected search results. The available transactions in the *Transaction* drop-down list are determined by the item type of the search results (for example *Delete Phone*, *Move Phone* and so on). The *Input type* drop-down list offers input source options for the transaction:

- If *screen* is selected, the transaction will be carried out on the selected search results.
- If *Excel file* is selected, a new *Input Data* group of controls is shown. The *Required file columns* list shows identifier columns that should be on the spreadsheet - see: [Bulk Administration file formats on page 520](#). The list of columns - required (in red) and optional - are shown according to the selected transaction in the *Transaction* drop-down list. Use the **Choose File** button to select the input file.

Note

An input file can also be loaded from the main Bulk administration screen - see: [Bulk Administration on page 516](#). While the use of an input file does not require the search results shown on the preview screen, a search on the item type is required to show the *Input Data* group of controls.

The *Select Execution Method* group of controls are used to carry out the selected transaction on the selected search result or input file according to the selected method - as on the main Bulk administration page. The drop-down list next to the **Execute** button provides three options:

- *Execute immediately*: the transaction will immediately be added to the transaction queue when the **Execute** button is clicked.
- *Schedule*: the transaction will be scheduled for execution at the date and time entered in the *Scheduled Date* and *Time* input boxes.
- *Export*: a *.xls* file is created in raw API format when the **Execute** button is clicked. No transaction is carried out.

The alternate button **Get Excel Identity Input File** creates a *.xls* file containing columns for the selected transaction and items - either selected from the search results or provided in another selected Excel input file. The default generated file name is *identifier.xls*.

Add input

For item types that allow Add transactions, the Bulk administration functionality supports this transaction separately. For the selected item (for example *Device* or *Phone*), an **Add** button is available on the page. Click the button to open the preview page containing an input form called *Specify RAW API user data*.

The form shows the selected *Item type* and *Selected Action*. Input controls and fields are available according to the item type and the transaction hierarchy as selected in the *Select Target* drop-down list. The *Add* group shows a *Count* input field that is used to enter the number of items to add. By default, this value is set to 1 and a single item can be added by means of this form. If the value is higher, then only a file can be generated and the drop-down list next to the **Execute** button only provides this option. Otherwise, the same three options are available as on the search results screen discussed above.

Use the **Generate Excel Identity Input File** button and these input controls to create a "template" Excel file that can be modified and used as an input file to bulk add items. The number of item rows that are added to the generated spreadsheet corresponds with the *Count* value. Columns are added for each field on the form and are populated with these values. The values entered on the form can be modified as required on the generated sheet. The Add action is also specified in a column on the Excel sheet - see [Bulk Administration file formats on page 520](#).

Bulk Administration file formats

Two types of files can be created from the Bulk administration screen:

1. Identity input files

Input files can be created (and then optionally modified) from the preview screen of search results or else manually as a MS Excel `.xls` file. These types of files can also be loaded as part of a search on the main screen or to specify a list of items on the preview screen for which an action is to be carried out.

The format of valid files is as follows:

- The first column can contain the transaction and entity type (green column headers). If present, it will always be in the following format:

```
action:<entity type>/<transaction type>
```

If the *Use file defined* option is selected from the *Action:* drop-down list in the *Execute a file* group of the main *Bulk administration* screen, the specified action will be carried out on the rows below the action.

Note

An input file can contain more than one action. Such a file can be created by combining files generated from the Bulk administration screen. For a valid input file, the actions will be carried out in sequence on the item rows below it if the *Use file defined* option is executed. If other options are selected to be executed, only the selected action will be carried out on the item rows below that action in the input file. No action will be carried out on other item rows in the input file.

- All input files require at least identifier columns marked with red column headers. They are the minimum information necessary to find the entity in the system. In addition, they may or may not include transaction information.
- Transaction columns (white column headers). They may or may not be compulsory (usually they are).
- Extra-info / Helper columns (yellow column headers) These are not needed by Bulk administration at all, but are merely included for the user's benefit, in aiding to identify extra information. Thus, even if the user were to change the values in this column to anything imaginable regardless of it being valid, Bulk administration will still ignore and disregard that as input.

2. Raw API files

When the *Export* method is selected for an execution method on the preview screen, this type of file is created. This file type is in the format to be used for API transactions with standard bulk loading tools in the system.

Common Bulk Administration tasks

This section describes common bulk administration tasks and the broad steps to carry these out. These tasks are carried out on the main screen (see: [Bulk Administration on page 516](#)) and the preview screen (see: [Bulk Administration Preview and Add on page 518](#)), where the controls to carry out the tasks are described (see below).

Common Tasks

Tasks described under this heading include basic bulk administration tasks.

Procedure

Searching for entity items and performing an action on one or more items in the search result list

- Step 1** Search for the items on the main screen.
- Step 2** Select a transaction to perform on the results on the preview screen.
- Step 3** Fill in the necessary transaction input information required for successful transaction completion on the preview screen.
- Step 4** Carry out the transaction on all the selected results on the preview screen.
-

Procedure

Searching for entity items and saving the results to a transaction input file

- Step 1** Search for the items on the main screen.
- Step 2** Select a transaction to perform on the results on the preview screen.
- Step 3** Generate an input file from the results.
- Step 4** Prepare the generated input file by filling in the remaining transaction information in order for the transaction to be successful.
- Step 5** Save the prepared input file for later use.
-

Procedure

Using multiple transactions on one input file

- Step 1** Repeat the typical procedure to create input files above several times for multiple (different) outputs (e.g. Add Phone, followed by Move Phone).
- Step 2** Combine the output of each generated input file into a single transaction input file (e.g. by using copy/paste) so that one single Excel sheet may contain several transaction steps that follow each other in sequence.
- Step 3** Save the combined input file containing multiple transactions - this sequence of transactions can be interpreted and then executed.
-

Procedure

Using an input file to repeat a search

- Step 1** Reload the list of saved entities contained in an input file on the main screen so that the same search results will be repeated on the preview screen as before (i.e. load as an input file the file that was originally generated).
- Step 2** The same results list that was displayed and used then to generate this input file can again be regenerated on the results screen by using the saved file to search with.
-

Procedure

Using the advanced search method to restrict results to a previous set of results

- Step 1** Use the main screen to combine the two search methods (Quick search and input file, to obtain a refined search result.
- Step 2** Use the Quick Search Filters to restrict the search to the subset of items contained in the input file.
-

Procedure

Directly executing transactions in a transaction input file

- Step 1** From the preview screen load a previously prepared transaction input file typically generated and prepared by using the procedures above or create such an input file manually, ensuring that the correct column structure is used to produce a valid input file.
- Step 2** Execute the loaded transaction input file
-

Procedure

Using search results to generate a raw-api file

- Step 1** Search for for items on the main screen.
- Step 2** Assign a transaction to the results on the preview screen and then save the transaction input file.
- Step 3** Load the saved file and select the execute method to export a raw-api file from the transaction and the item information contained within the input file.
- Step 4** If required, edit this raw API file manually (change/add to it).
- Step 5** Use this raw API file with the standard bulk loading tools.
-

Typical Bulk Administration Task Examples

Tasks described under this heading include typical bulk administration tasks for commonly used functionality (see below).

Modifying phone features

Note

- This bulk administration task will typically be performed only by an administrator, who should be familiar with bulk loading as well using Microsoft™ Excel®.
 - Phone features **can only be modified on registered phones**.
-

This bulk administration task allows users to update any of the following:

- Phone line features, namely any of the settings per line, such as private line settings or common line settings.

- General phone features, such as Button Template, Device Pool Name, Idle Timeout, Idle URL, and other fields found at the top of the *Phone Management* screen.

Procedure

Search and select phones

To search/select phones:

- Step 1** Select the *Phone* or *Device* option from the *Select item* drop-down list.
 - Step 2** Select the required target search hierarchy from the *Select Target* drop-down list. This effectively determines the location of the phones for which you want to modify the features.
 - Step 3** Select the required phone filter details, for example Device Name, Phone Type, and so on to determine which phones to include in the list. For example, to select all Cisco 6941 phones at the location, select the *Phone Type* option, select the *Contains* option, and then enter *6941* in the associated text field. Select the *add* active text link, and repeat this process as many times as required to include the required filter details. Select the *del* active text link if required to remove the associated filter details.
 - Step 4** Click the **Search** button when complete. A list of phones that match the search criteria is displayed.
 - Step 5** Select the required checkboxes to select the actual phones to update. To select all phones, select (enable) the checkbox at the top of the list (adjacent to *Provider Name*).
-

Procedure

Modifying features

To modify multiple phone details and line features for the selected phones (see section above):

- Step 1** Select the *Modify Phone Features* option from the *Transaction* drop-down list.
- Step 2** Select the *Screen - Single value per column* (default) option from the *Input type* drop-down list. An input data form is displayed, allowing you to enter/modify the following phone details/line features:
 - Line
 - LineFeature
 - LineFeature Value
 - Phone Description *
 - Button Template *
 - Device Pool Name *
 - Idle Timeout *
 - Idle URL *
 - Language *
 - Media Service *
 - SIP Profile Name *

Note

The Line fields (Line, LineFeature and LineFeature Value) collectively represent **one line feature**. The remainder of the fields (denoted with an '*') show the general phone features that can be modified (in the current version of the CUCDM bulk administration feature).

Step 3 Enter one or more values into the input data form field/s displayed in the above step.

Note

Values entered into the LineFeature field must be entered in exact qxml tag name form, and **not** entered as displayed on the *Phone Management* screen. For example, Alerting Name must be entered as 'AlertingName', Alerting name ASCII must be entered as 'AlertingNameASCII', and Display name (Caller Line ID) must be entered as 'DisplayName'.

Step 4 Click the *Get Excel Identity Input file* button. This generates and opens (depending on browser settings) an Excel spreadsheet listing all the phones and features. This spreadsheet effectively forms a template, which can be manipulated to modify as many phone/line features as required.

Step 5 Open the generated Excel spreadsheet (input file) - if it was not opened automatically.

Step 6 To prepare the Excel spreadsheet to modify multiple line features on multiple phones/lines, copy the three columns Line[1], LineFeature[1] and LineFeature Value[1], and paste them on the right of the LineFeature Value[1] column. This results in columns E, F and G, being Line[1], LineFeature[1] and LineFeature Value[1] respectively, and columns H, I and J also being Line[1], LineFeature[1] and LineFeature Value[1]. To cater for the second line feature, replace the [1] in columns H, I and J with a [2]. Repeat this process as many times as required to cater for/represent the required number of line features that you want to modify. When complete (to cater for 'n' line features), the Excel spreadsheet (columns E to S) would look something like this: Line[1], LineFeature[1], LineFeature Value[1]....., Line[n], LineFeature[n], LineFeature Value[n]. See below for an example showing two line features.

D	E	F	G	H	I	J	K
LineFeaturesCount	Line[1]	LineFeature[1]	LineFeature Value[1]	Line[2]	LineFeature[2]	LineFeature Value[2]	Phone
2	1	RingSettingPhoneActive	Ring Once	1	Label	TestLabel	Edit

Step 7 As previously mentioned, the Line[1], LineFeature[1] and LineFeature Value[1] columns represent **one** line feature. Enter a valid line feature to modify in the LineFeature[1] field for example *RingSettingPhoneActive*, and then enter a valid corresponding value in the LineFeature Value[1] field, for example *Ring Once*. Enter valid values for Line[2], LineFeature[2] and LineFeature Value[2] to modify the second line feature, etc. Repeat as many times as required.

Step 8 After modifying the phone/line features for each required line, set each of the *LineFeaturesCount* column (located to the left of the *Line[1]* values to match the total number of line features, for example if you wanted to modify two line features as shown in step 5, then the corresponding *LineFeaturesCount* value must be set to '2'.

Step 9 Save the modified Excel input file.

Note

The Excel input file can be uploaded and executed from either the *Bulk Administration search screen* or the *Bulk Administration search results screen* (see below):

Procedure

Upload and execute the modified Excel input file - from the Bulk Administration - Search screen:

Step 1 Click the **Choose File** button, navigate to the required Excel input file and click the **Open** button.

- Step 2** Click the **Execute** button.

Procedure

Upload and execute the modified Excel input file - from the Bulk Administration - Search results screen:

- Step 1** Select the *Excel file* option from the *Input type* drop-down list.
- Step 2** Click the **Choose File** button, navigate to the saved Excel input file and click the **Open** button.
- Step 3** Click the **Execute** button.

Note

Refer to [Bulk Administration Preview and Add on page 518](#) (if required) for more information about executing/scheduling the Excel input file.

Summary

Upon executing the Excel input file, note the following:

- Each item (line) in the Excel input file represents one transaction, and all transactions will run in sequence.
- If all transactions succeed, the phone/line details are modified accordingly. Check the relevant *Phone Management* screen to view the relevant changes if required.
- If a validation error occurs, re-open the Excel input file, repair/update the file if possible and run the upload/execute process again. Contact your local support representative for assistance if required.

IVR/Transit Server Management

For basic IVR server management, see: [IVR Server Management on page 137](#).

An IVR Server can be associated with a Transit Server(s).

Procedure

Viewing Associated Transit Servers

To view Transit Servers currently associated to the selected IVR Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **IVR Server==>Transit Server** button adjacent to the IVR Server that you would like to view.

A screen will be displayed, with two columns, one listing the registered (and available) Transit Servers, and the other column will display the Transit Servers current connection status. If the button adjacent to the Transit Server says **Connect**, the Transit Server is available for connection. If the button says **Disconnect**, the Transit Server is already connected.

Procedure

Associating (connecting) an IVR Server to a Transit Server

To associate a IVR Server to a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **IVR Server**==>**Transit Server** button
- Step 3** Select the **Connect** button Adjacent to the Transit Server that you would like to associate with the IVR Server.

The IVR Server will now be associated with the selected Transit Server.

Procedure

Disassociating (disconnecting) an IVR Server from a Transit Server

To disassociate a IVR Server from a Transit Server:

- Step 1** Browse to the relevant section under the *Network* menu
- Step 2** Select the **IVR Server**==>**Transit Server** button
- Step 3** Select the **Disconnect** button adjacent to the IVR Server that you would like to disassociate from a Transit Server(s).

The IVR Server will now be disassociated from the selected Transit Server.

Transaction Auditing

Transaction Auditing consists of three parts - the management section, the framework and the audit application.

The management section is used to configure and enable or disable the framework while the audit application is used to search for and view transaction and audit details.

Management of Transaction Auditing

Transaction Auditing is a powerful tool that enables administrators to closely monitor all or specific transaction types processed within the system.

Auditing consists of two core parts, a management framework and the actual audit application. The management section is used to configure and manage the audit functionality and the actual audit application is used to view transactions and other audit information.

Important

- Only system administrators can manage and configure the audit framework and grant access to the audit application. System administrators have access to the audit application by default. Only administrator roles (from Provider down to Location) can be granted access to the audit application. Access is granted to the Auditing functionality via the *Audit* option in Access profiles. For standard auditing functions, assigning a user read rights to this option is sufficient. For more information on Access profiles, please see the Access Profiles topic.

- Depending on the configuration of your system, enabling auditing may degrade the performance of the system. It is normal for transactions to take longer to process when auditing is enabled compared to when auditing is disabled, this is due to the added processing steps required by the auditing functionality.

Procedure

Configuring the System for Transaction Auditing

Before the transaction auditing functionality can be utilized, the functionality needs to be enabled and configured within the system. Follow the steps below to activate transaction auditing within the system:

- Step 1** Browse to *Setup Tools > Global Settings*.
- Step 2** Select the *AuditTransactions* option.
- Step 3** Select the *Current Setting* checkbox to enable Auditing.
- Step 4** Click the **Modify** button to activate auditing.

Auditing is enabled in the system.

For more information on using system tools, please see [System Preference and Settings on page 946](#).

Procedure

View and Modify the Transaction Auditing Configuration

Follow the steps below to configure Transaction Auditing within the system:

- Step 1** Browse to *Setup Tools > Audit*.
- The transaction auditing page displays the current auditing configuration and lists all of the actions currently available for auditing, as well as their current auditing status. The Audited Attributes column displays the number of attributes that are currently flagged for auditing for each action.
- Step 2** To enable or disable auditing actions, **select or deselect** the relevant checkbox in the *Audit Status* column then click the **Modify** button.
- Step 3** Select the *Action* (active text link) that you would like to modify.
- Step 4** Make the required modifications and click the **Modify** button.

The audit configuration is updated in the system.

The following fields are available when modifying an Action:

Field	Description
<i>Action Name</i>	This is the name that the system uses to refer to the action. This field cannot be modified by the user on this screen.
<i>Action Display Name</i>	A "friendly" name for the action that is displayed in the list. This is a mandatory field.

Field	Description
<i>Audit Status</i>	Select this checkbox to activate auditing for this feature, deselect the checkbox to de-activate auditing for this feature.

Procedure

Configuring Attributes

The attribute page enables administrators to change the display name that end-users of the audit application see next to audited attributes, as well as to modify the behavior of specific audit attributes.

To configure attributes:

Step 1 Browse to *Setup Tools > Audit*

Step 2 Select the *Action* (active text link) that you would like to modify.

Step 3 Click the **Configure Attributes** button.

This page lists all of the available attributes, the list includes the Attribute Name, Display Name, Enabled (Attribute Status), and Visible (Select to mask values).

Step 4 Make the required changes to the attributes and click the **Modify** button.

The audit configuration is updated in the system.

Note

To load suggested default settings for the page, click the **Load Defaults** button.

The following fields are available when editing an attribute:

Field	Description
<i>Attribute Name</i>	This is the name that the system uses to refer to the action. This field cannot be modified by the user on this screen.
<i>Display Name</i>	A "friendly" name for the action that is displayed in the list. This is a mandatory field.
<i>Enabled</i>	Select this checkbox to activate auditing for this attribute, deselect the checkbox to de-activate auditing for this feature.
<i>Value Visible</i>	This checkbox determines if a value is obscured (masked) by the audit application. Enabling this feature for attributes containing sensitive data such as passwords and account numbers is recommended.

Transaction Auditing Application

Transaction Auditing is a powerful tool that enables system administrators to closely monitor all or specific transaction types processed within the system.

Important

Before using the Audit Application, please ensure that Auditing has been correctly configured. Please see [Management of Transaction Auditing on page 526](#) for further information.

Procedure

Accessing and Using the Audit Application

Step 1 The Audit Application is accessed using a web browser via the hyperlink: *https://<your-platform-ip>/audit/*, where *<your-platform-ip>* is replaced with the base URL of your system. For example, if the system is accessed via the URL: *https://1.2.3.4/bvsm/*, auditing is accessed via the URL: *https://1.2.3.4/audit/*.

Step 2 Log in with your user name and password.

Note

Please ensure that your current user level includes access to the Audit Application. If you are not able to access the Audit Application, please contact your organization's administrator who is responsible for user accounts and access profiles.

Step 3 The application page enables you to search for transactions based on a combination of transaction-related criteria or criteria related to the actual objects that were affected.

To search for transactions based on transaction-related criteria, enter your search criteria in the *Transaction criteria* text field

To search for transactions that affected specific audited objects, enter your search criteria in the *Audit Parameters* text field

Once you have entered your required search criteria, click the **Search** button.

The search results are returned and you can browse through the results and view the audit details.

Note

A history list enables you to return to previous search results without having to resubmit previous searches.

Important

- You cannot browse any search results that involve objects outside of your own security level. These transactions are marked as *restricted* in the search results grid. For example, a user who does not have access to Branding functionality, can not view any search results that include Branding related objects.
 - Transaction search results for user related transactions that fall outside of your security level, have their user name and message fields obscured (masked) as this information is deemed sensitive.
-

Transaction Details

The transaction details page displays a range of details for the selected transaction and is divided into three sections, Transaction Detail, Sub-transactions and Audited Changes.

The details displayed include:

Note: Depending on whether the transaction is a sub or main transaction, available fields may differ.

Field	Description
<i>Request ID</i>	The unique ID of the transaction

Field	Description
<i>Parent Request ID</i>	Displayed for sub-transactions only, this field contains the transaction number of the main (parent) transaction that triggered the transaction being viewed.
<i>Timestamp</i>	The date and time that the transaction was processed
<i>Action</i>	The key action that was taken by the transaction. For example, "ModPerson" would signify that the core function of the transaction was to modify a users details.
<i>Executed By</i>	The username of the user that ran the transaction (the user who was logged in to the system when the transaction was executed).
<i>Status</i>	The status of the transaction. "Y" means the transaction succeeded while "F" means the transaction failed.
<i>Messages</i>	A message summarizing the result of the transaction, for example, " New User Added" or "Invalid email address". This message is the same message that is displayed in the system once the transaction has completed.

- Sub-transactions

This section displays a list of all the sub-transaction related to the main transaction being viewed. Selecting a sub transaction displays the details of the sub transaction. Sub-transactions are selected by selecting any part of the sub-transaction's row (active text link).

- Audited Changes

This section lists all the specified audit objects that were affected by transactions. To search purely for audited changes, use the Audit Parameters section to search for transactions.

Important

- You cannot browse any search results that involve objects outside of your own security level. These transactions are marked as *restricted* in the search results grid. For example, a user who does not have access to Branding functionality, can not view any search results that include Branding related objects.
 - Transaction search results for user related transactions that fall outside of your security level, have their user name and message fields obscured (masked) as this information is deemed sensitive.
-

Billing Codes (Client Matter Codes)

Client matter codes are known within the system as billing codes. Throughout this document client matter codes will be referred to as billing codes. Administrators should be using the system administration to configure the codes [client matter codes will only be referred to when configuring Cisco Unified Communications Manager (Unified CM) directly].

To use the billing code feature, users must enter a billing code to reach certain dialed numbers. Users can enable or disable billing codes through the system administration, control route patterns, and configure multiple billing codes. When a user dials a number that is routed through a billing code enabled route pattern, a tone prompts the user for the code. When the user enters a valid billing code, the call occurs; if the user enters an invalid code, reorder occurs. The billing code writes to the CDR, so users can collect the information by using CDR Analysis and Reporting (CAR), which generates information for client accounting and billing.

In Unified CM administration, users must enable CMC for new or existing route patterns. After configuring CMC, it is essential to update dial plan documents to indicate the billing code route patterns.

Planning

For a successful deployment of billing codes planning should begin at the very early stages of a deployment. As the billing code functionality is directly related to route patterns within Unified CM, an agreement on whether a customer requires this functionality should be determined before provisioning.

If a customer requires billing codes after they have been deployed, then a number of manual steps are required. As this is a direct manual configuration on the Cisco Unified Communications Manager, the system has no knowledge of this configuration and so cannot manage it.

Setting up Billing Codes

Users can enter billing codes in system administration or through the bulk loaders. To add, assign, disable or update billing codes, the following procedures must be performed:

To add a billing code range, browse to *Resources > Billing Codes* and select the *Add Range* option.

Available fields include:

Field	Description
Start billing reference code	<p>Enter a unique billing code range number no more than 16 digits that the user will enter when placing a call. Currently the system allows billing reference codes of a maximum of 16 characters in the following formats:</p> <ul style="list-style-type: none"> Any numeric code, e.g. '1234567890123456'. Any numeric code with leading 0's, e.g. '0123456789012345' or '000123'. Any numeric code containing decimals. In this scenario, the code is formatted to drop all digits after the decimal and prefix the code with 0's up to the length of the original code containing the decimal value. <p>Therefore, if you had '123.456' as a code, the formatting would change it to '0000123'. In other words, the original code ('123.456') was 7 characters long. The decimal and everything following it are removed, which leaves you with a 3 digit number '123'. Because the original code contained 7 characters, four 0's are prefixed to the code which gives you '0000123'.</p>
Description	Enter a name of no more than 50 characters. This optional field associates a billing code with a client.
Range size	Select a range. This will determine how many billing codes will be created from the starting billing code number.

Assigning Billing Codes to Customers

Once billing codes have been created successfully, they need to be assigned. Billing codes can be assigned to resellers, customers, divisions, locations and users. To successfully use billing codes they need to be finally assigned to a user. The system gives administrators the ability to reserve ranges for customers and later allocate them to users.

To add a billing code range, browse to *Resource > Billing Codes > Assign Range* then click the **Next** button.

Field	Description
Assignment to billable type	Select Resellers, Customers, Divisions, Locations or User.

Field	Description
Start billing reference code	<p>Enter a unique billing code name no more than 16 digits that the user will enter when placing a call. Currently the system allows billing reference codes of a maximum of 16 characters in the following formats:</p> <ul style="list-style-type: none"> Any numeric code, e.g. '1234567890123456'. Any numeric code with leading 0's, e.g. '0123456789012345' or '000123'. Any numeric code containing decimals. In this scenario, the code is formatted to drop all digits after the decimal and prefix the code with 0's up to the length of the original code containing the decimal value. <p>Therefore, if you had '123.456' as a code, the formatting would change it to '0000123'. In other words, the original code ('123.456') was 7 characters long. The decimal and everything following it are removed, which leaves you with a 3 digit number '123'. Because the original code contained 7 characters, four 0's are prefixed to the code which gives you '0000123'.</p>
Range size	Select a range, which determines how many billing codes will be reserved for that level.

Procedure

- Step 1** To add a billing code range, browse to *Resource > Billing Codes > Assign Range > User* and click the **Next** button.
- Step 2** The system will then request a filter down to an end user.
- Step 3** Click the **Assign Range** button.

Billing Codes and the CCM Model

When a location is created in the system, the route patterns are determined by the CCM model. It is important to make sure that the route patterns have Client Matter Codes (CMC) enabled. It is possible to provision normal route patterns and CMC enabled route patterns for the same location using the CCM model. This is the preferred and supported method, and enables billing codes using the COS at the feature group level. Separate COS will be required to support billing codes.

When setting up route patterns within the CCM model the following needs to be activated: *Enable Client Matter Codes*. This will enable the billing code feature.

Manually Configuring Billing Codes on Provisioned Locations

The system provisions route patterns when adding a location. In the instance where a location has been added and at a later date a customer decides they need the billing code feature, the following needs to be considered:

- If all users require billing codes then amend the current route patterns for that location and check the Require Client Matter Code box.
- If a customer would like a mixed environment then copy the existing route patterns and enable the matter codes on the desired route patterns. It must be understood that when adding route patterns manually, system administration has no knowledge of them.
- This method needs to be taken with extreme care as from this point the management of route patterns has to be done via Cisco Unified Communications Manager administration. Partitions and calling search spaces will also need to be manually configured.

Procedure

To manually add CMC enabled route patterns:

Step 1 A new partition and calling search space will be required per route pattern.

Note

We recommend that you copy existing calling search spaces and rename them. Add CMC in the name. Manually add the partitions per call type. We advise that you use the current naming convention.

Step 2 In Cisco Unified Communications Manager administration, browse to *Call Routing > Route/Hunt > Route Pattern*.

Step 3 Perform one of the following tasks:

- **To update an existing route pattern:** enter search criteria in the 'Find and List Route Pattern' window, as described in [Route Pattern Configuration](#)² in the Cisco Unified Communications Manager Administration Guide.
- **To add a new route pattern:** refer to [Route Pattern Configuration](#)³ in the Cisco Unified Communications Manager Administration Guide.

Step 4 In the Route Pattern Configuration window, check the Require Client Matter Code checkbox.

Step 5 Perform one of the following tasks:

- If you updated the route pattern, click the **Save** button.
- If you added a new route pattern, click the **Save** button.

Note

Copying existing route patterns, renaming them, and enabling CMC is recommended.

Step 6 Manually change the *Calling Search Space* per phone.

Billing Summary

It is important that billing codes are included in the early design process. Adding billing codes after a location has been added can cause a number of issues, particularly as the system has no knowledge of the manually added configuration done via Cisco Unified Communications Manager administration.

The following must be understood before adding Billing Codes manually, after a location has been provisioned:

- System administration will not be able to control the phone. Administrators will not be able to enable or disable the billing feature via the feature group
- System administration will not be able to delete the location as it has configuration it is unaware of.
- Extreme care has to be taken when manually configuring Cisco Unified Communications Manager

It is acknowledge that a new feature enhancement is required to be able to manage route partition, partitions and calling search spaces at the location level to ensure that the system is aware and can manage them. This is a road mapped feature.

² http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/5_1_3/ccmcfg/b03rtpat.html#wpixref28844

³ http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/5_1_3/ccmcfg/b03rtpat.html#wpixref28844

Quick Search

Note

The use of wildcards in search criteria can lead to unexpected results and should therefore be avoided.

Each page of the system user interface includes a Quick Search link, which allows you to search the system for specific entries, including phones, extensions, and user accounts. The Quick Search page provides a quick and efficient search mechanism for entries of various types from a single page in the system without the need to navigate up / down the system hierarchy tree via the menu. The Quick Search options and results to which you have access are determined by the access privileges associated with the user account that you used to log into the system.

The Quick Search icon appears as an Active Text called **Quick Search**, at the top right hand side of all GUI pages.

When you select the *Quick Search* link, the system displays a page which displays a list of the entries in the system to which you have access.

Search For

Select the required option from the *Search For* pull-down selection list to identify the type of entries for which you want to search and select the *Search* button.

The following table provides a brief description for the options available for search via Quick Search:

Search Type	Description
Location Searches	
<i>Location</i>	Find a location by name.
<i>Location with Site Code</i>	Find a specific location by entering the site code.
<i>Location of User</i>	Find a location by entering a user account name.
<i>Location of Phone</i>	Find a location by entering the Device Name of a phone.
Extension Searches	
<i>Extension</i>	Find an extension by its number.
<i>Extension associated with DDI</i>	Find an extension by entering the external line to which it is registered.
<i>Extension used by User</i>	Find an extension by entering the associated user.
<i>Extension used by Phone</i>	Find an extension provisioned on a phone by entering the Device Name of the phone.
Phone Searches	
<i>Phone with Extension</i>	Find a phone by entering the associated extension.
<i>Phone with DDI</i>	Find a phone by entering the external line number of the phone.
<i>Phone with User</i>	Find a phone by entering the associated user account name.
User Searches	
<i>Username</i>	Find a user by entering the user name.
<i>Surname</i>	Find a user by entering the last name of the user.
<i>Firstname</i>	Find a user by entering the first name of the user account.
<i>User with Extension</i>	Find a user by entering the extension associated with it.

Refined Search

On the Quick Search page, various options are available to the User to refine their search. These options are explained in more detail below.

Search By

To refine your search, select one of the following options from the *Search By* pull-down selection list. Use this field when you have additional information available pertaining to your search.

- **Pattern ends with:** Enter the last few characters of the entry that you want to find.
- **Pattern starts with:** Enter the first few characters of the entry that you want to find.
- **Pattern includes:** Enter any string that is included in the entry that you want to find.

The use of *Search By* pattern in conjunction with the additional information field refines the search and reduces the number of entries in the result screen, thus allowing you to get to your target entity faster.

For example a part of a phone extension number can be typed in the additional information field when using the *Search for* option.

Max Results

To specify the number of entries you want the system to display on a single page, select the number from the *Max Results* pull-down selection list.

Note

The use of *unlimited* for should be considered very carefully. A search with no refined criteria and unlimited numbers results, may take very long time to present.

At the bottom of the results screen, the system will provide you with information about the total number of records found for your search, the number it shows on the screens so far and buttons to present the next and / or previous screen.

Current Context

If the *Search in Current Context* checkbox is selected, the Quick search will be done only in the current entity and below.

For example, searching for users in context while in a location will present only the users in the location. However, the same search without Context will present all the users in the system.

Finding Locations

Location (Name)

When searching for details of a location by its name and you are unsure of the exact details of it select *Location* from the drop-down list in the *search for* option with no specific additional information and a list of all Locations will be displayed.

However, if you know the full name of the location (or part thereof), select *Location* from the drop-down list in the search for option and enter the known details in the additional information search field - details pertaining to your query will be displayed.

Note

If you are using the additional information field to refine your search for the location, note that the system uses this information with regards to the location name only.

Location with Site Code

If you know the Location Site Code (or part of it), use the *Location with Site Code* option and enter the site code in the additional information search field - this will display all the locations relevant to your search.

Select the required Location from the list by selecting the Location (active text link - marked by a different color) under the Location Name; this will take you directly to the Manage Location page.

Location of User

If you know the name of a user (or part of it) but are unsure of the Location details, use the *Location of User* option and enter the user name in the additional information field - this will display all the Locations relevant to your search.

Note

This search allows you to refine by specifying all or part of the User only.

Location of Phone

If you know details of the Phone but are not sure of its location, use the *Location of Phone* option and enter the details of the Phone (or part of it) in the additional information search field - this will display all the Locations relevant to your search.

Find Location in the List

When presenting the search result list of locations in Quick Search, the system shows the full location path with ":" separating the levels in the hierarchy. Therefore, the location details are displayed as follows: Provider , Reseller , Customer , Division and Location.

Additionally, the system shows the location address.

Once you get the list of locations, select the required location by selecting it (active text link) in the list. This will take you directly to the *Manage Location* page.

Finding Extensions

An extension search displays a list of Internal Extensions (Numbers) in the system.

Extensions

Use the Extension search option from the drop-down list in the *search for* when the only information available to you is the Internal Extension (number) of a phone or a user or part of it. A list of all the extensions available in the Provider, Reseller, Division, Customer and Locations will be displayed.

Note

As you will see from the screen above, the search will produce a large amount of data. It is highly recommended to refine your search by including as much detail as possible using the *Search By* and the additional information fields should you have additional information available. In case the platform you are using has a large number of available (even if not allocated) internal extensions an unrefined search might result in a very large list of extensions which will take long to display.

Extension associated with DDI

When searching for an extension and you know the associated DDI number (or part of it), select *Extension associated with DDI* from the drop-down list in the *search for* option and enter the DDI details you have in the additional information field. The result will display all the extensions applicable for the DDI/PSTN details provided.

Extension used by User

When searching for an extension and you know the User name, select *Extension used by User* from the drop-down list in the *search for* option. Enter the name of the User (or part of it) in the additional information field and a list of all extensions associated to the users answering the search criteria will be displayed.

Note

The list of results will provide all the extensions linked to a user answering to the search criteria. These can be extensions set for user extension mobility profile or for phones which are associated with users.

Extension used by Phone

When searching for an extension, and you know the phone name (or part of it), select the *Extension used by phone* option from the *search for* drop-down list. Enter the phone details in the additional information field and a list of all extensions relevant to the phone type will be displayed.

The search result will present a list of extensions provisioned to phones that corresponds with the additional information details of the search.

Find an Extension in the List

When presenting the list of Extensions in Quick Search, the following details are available for any Extension displayed:

Field	Description	Remarks
Internal Number	The extension number.	<p>Active Text Links:</p> <ul style="list-style-type: none"> • Allow: Number is not available for the location and cannot be used currently. Selecting the active text link will make the number available for use In the location • Prevent: Number is available in the location and can be used. Selecting the active text link will make the number unavailable for use in the location. • When a number is available it means that it will show up in a drop-down list when user (usually admin user) needs to use an extension (for example, when registering a phone or adding an Extension Mobility Profile to an end user).

Field	Description	Remarks
Associated PSTN Number	The DDI (E164/DID) linked to the internal extension.	This is a read-only field.
Hunt Group	If the extension is part of a Hunt Group the name of the Hunt Group will be displayed.	This is a read-only field.
Pickup Group	If the extension is part of a Pickup Group the name of the Pickup Group will be displayed.	This is a read-only field.
Class of Service	Defines the permissions an extension will have.	This is a read-only field. In case the number is used by a registered phone or for user extension mobility profile.
Used by	Information about where the extension is found and what to (if applicable) it is linked to.	This is a read-only field. Information is presented in the following structure: Provider : Reseller : Customer : Division : Location: YYYY:XXX <ul style="list-style-type: none"> • YYYY: The user name whose extension mobility profile is set with this extension. • XXX: USER if the extension is linked to user extension mobility profile.

Finding Phones (Device Name)

Each phone has a unique device name that enables it to be controlled on a network. The device name is always unique to the device. Device name searches display a list of the relevant phones registered in the system.

Note

Currently only registered phones are available for the device name search types.

Phone with Device Name

When searching for a phone and you have the Device Name (or part of it) of the device, select the *Device Name* Search option from the drop-down list in the *search for* option. Enter the details of the device name in the additional information field and click **Search**. This will display a list of all the phones that correspond to the additional information field.

Note

See [Find a Phone in the List on page 539](#) if required for a detailed description of the information displayed in the result list fields.

See also:

- [Phone with Extension on page 539](#)
- [Phone with DDI on page 539](#)

- [Phone with User on page 539](#)
- [Find a Phone in the List on page 539](#)

Phone with Extension

When searching for a phone and you have the extension number (or part of it) of the phone, select the option *Phone with extension* from the drop-down list in the *search for* option. Enter the details of the extension in the additional information field and click **Search**.

This will display a list of all the phones which are registered with an extension number that corresponds with the details provided in the search criteria.

The *Phone with Extension* option is the default search option presented when you select *Quick Search*.

Note

See [Find a Phone in the List on page 539](#) if required for a detailed description of the information displayed in the result list fields.

Phone with DDI

When searching for a phone and you have the DDI number (or part of it) of the device, select the *Phone with DDI* option from the drop-down list in the *search for* option. Enter the DDI number in the additional information field and click **Search**. This will display a list of all the Phones which are registered with a DDI number corresponding with the details provided in the additional information field.

Note

- The results screen does not present the DDI allocated to the phone.
 - See [Find a Phone in the List on page 539](#) if required for a detailed description of the information displayed in the result list fields.
-

Phone with User

When searching for a phone and you have the details of the user associated with it (or part of the user details), select the *Phone with User* search from the drop-down list in the *search for* option. Enter the User in the additional information field and click **Search**. This will display a list of all the phones which are associated to users corresponding with the details provided in the additional information field.

Note

See [Find a Phone in the List on page 539](#) if required for a detailed description of the information displayed in the result list fields.

Find a Phone in the List

When presenting the list of Phones in Quick Search, the Device Name presented in the list is an active text link (marked by being in a different color and changing the look of the cursor when it hovers over it). When selected, the system will take you directly to the *Phone management* page for the phone.

The following details are available for any phone displayed:

Field	Description	Remarks
Phone Type	The Phone Type allocated in the system to this Device Name when the phone was added to the Inventory.	This is a read-only field.
Device Name	The device name of the actual phone.	Active text link: Selecting the Device Name will open the phone management page for this phone.
First Line Ext/Label	Extension number and the line label for it.	This is a read-only field. Line label displayed only if different than default.
Description	Details of the Provider, Reseller, Division, Customer and Location of the Phone.	This is a read-only field. Position is the point in which the phone is installed. It is optional information added at the point of registration of the phone.
Configuration Profile	Marks if the phone is a real phone (actual handset) or a fake phone.	This is a read-only field. <ul style="list-style-type: none"> • N (Default): Real phone • Y: A phone marked with configuration profile flag. Such phones are used mainly for Phone Based Registration.
Associated User	The user with whom the device is associated.	This is a read-only field. None if the phone is not associated with any user.
IP Address	The IP address of the phone.	This is a read-only field.
Service Status	Details of the phone status.	Active text link: <ul style="list-style-type: none"> • In Service: Device available for service. This is the normal operational mode. Selecting the active text link will take the phone Out of Service. • Out of Service: Device not available for service and cannot be used currently. Selecting the active text link will put the phone back into In Service mode. • Partially out of service(limited calling options): If the first line of the phone is suspended (using Operations Tools/"Suspend All Phones At Location Out of Service/First Phone Line Only" checkbox), then the first line of the device is not available for service and cannot be used currently. Selecting the active text link will put the phone back into In Service mode. <p>Note</p> <ul style="list-style-type: none"> • After running the Ops Tool with the <i>First Phone Line Only</i> checkbox selected, then unsuspending the phone from the phone management page, if you then resuspend the phone, a full out of service is triggered, not the first line only. • If a first line suspend is run directly after a full suspend, only the first line on the phone is suspended.

Finding a User

User search is for cases in which the details you have are of a user and you are looking to identify it and/or get to manage the user information.

User Name

When searching for a user and you have the Username (or part of it), select the *Username* option from the drop-down list in the *search for* option. Enter the Username in the additional information field and click **Search**. This will display a list of all the users whose username correspond with the details provided in the additional information field.

Surname

When searching for a user when you have the User's Surname (also known as Last name) or part of it, select the *Surname* option from the drop-down list in the *search for* option.

Enter the user's Surname in the additional information field and click **Search**. This will display a list of all the users with a last name that corresponds with the details provided in the additional information field.

First Name

When searching for users while you have the User's First Name (or part of it), select the *First name* option from the drop-down list in the *search for* option. Enter the user's first name in the additional information field and click **Search**. This will display a list of all the users with a First Name that corresponds with the details provided in the additional information field.

User with Extension

When searching for user details and you have the user's (internal) extension number (or part of it), select the *User with Extension* option from the drop-down list in the *search for* option. Enter the extension details in the additional information field and click **Search**. This will display a list of all the users with an extension that correspond with the details provided in the additional information field. The extension can be of a user extension mobility profile or of a phone associated with the user.

When searching for user details which you know is associated with a phone and you have details of the phone device name (or part of), select the *User with Phone* option from the drop-down list in the *search for* option. Enter the Device name details in the additional information field and click **Search**. This will display a list of all the users associated with phones where the device name correspond with the details provided in the additional information field.

User with DDI

When searching for user details while you have the User's DDI number (or part of it), select the *User with DDI* option from the drop-down list in the *search for* option. Enter the DDI number details in the additional information field and click **Search**. This will display a list of all the users with DDIs which correspond with the details provided in the additional information field.

Note

The DDI can be linked to a user extension mobility profile or to a phone associated with the user.

Find a User in the List

When presenting the list of Users in Quick Search, the following details are available for users:

Field	Description	Remarks
Username	The User Name is a unique name or number created to identify each individual user.	Active text link. Selecting the username active text link will open the User Management screen for it.
Name	The first name and last name of the user	This is a read-only field.
Location	Details of the Provider, Reseller, Division, Customer and Location of the User.	This is a read-only field. Information is presented in the following structure: Provider:Reseller:Customer:Division:Location
Associated Device(s)	Details of the phone associated with the user.	This is a read-only field.
Voicemail	Indicates if User has access to Voicemail.	Active text link: <ul style="list-style-type: none"> • N/A: The user does not have access to Voicemail. • Add The user is allowed to have a Voicemail box, but does not have one yet. Selecting it will redirect you to the page where you can create a voicemail account. • Y: User has a Voicemail box set up. Selecting it will redirect you to the Voicemail management page for the user.

Field	Description	Remarks
Extension Mobility	Indicates if User has access to an Extension Mobility profile and if it is active or not in service.	<p>Active text link:</p> <ul style="list-style-type: none"> • N/A: the user is not allowed to have an Extension Mobility profile. • Add: The user can have an extension mobility profile, but it is not yet defined. When selecting Add, it will redirect you to the page where you can create an extension mobility profile for the user. • An extension number and In Service: A mobility profile has been set for this user and its status is in a normal operational mode thus all actions are available for this profile. Selecting the In Service active text link will change the extension mobility profile status to be Out of Service. • An extension number and Out of Service: An extension mobility profile has been set for this user and its status currently is "Out of Service". This means that the extension mobility profile is not active in and the user cannot use it for any activity. Selecting the Out of Service active text link will change the extension mobility profile status to be In Service.

Bulk and Model Loader Functionality

Note

For detailed information on Model and Bulk Loaders, refer to the Model Guide and the Bulk Loader Guide respectively.

Model Management

The *Model Management* page enables administrators to manage their dial plan configuration models, primarily the models route patterns and translation patterns.

Procedure

Managing Translation Patterns

To manage translation patterns within a particular model:

- Step 1** Browse to *Dial Plan Tools > Model Management*.

- Step 2** Select the *Manage Translation Patterns* active text link.
- Step 3** Select the *Dial Plan* (active text link) to modify.
- Step 4** Select the *Template* (active text link) to modify.
- Step 5** Select the *Model* (active text link) to modify.

The resulting page will list all translation patterns available for the selected dial plan, template and model. From this page you are able to add, modify, delete and apply translation patterns.

Procedure

Deleting a Translation Pattern

- To delete a translation pattern, select the check-box adjacent to the relevant translation patterns then click the **Delete Selected** button.

The translation pattern will be removed from the dial plan.

Procedure

Modifying a Translation Pattern

- To modify a translation pattern, select the *name* (active text link) of the translation pattern that you would like to modify, make the required modifications then click the **Modify** button.

The translation pattern will be updated within the system.

Procedure

Adding a Translation Pattern

- To add a translation pattern, click the **Add** button, complete all of the required fields, then click the **Add** button.

The translation pattern will be added to the Dial Plan.

The following fields are available:

Field	Description	Remarks
Specific Information		
Dial Plan Name	Name of the selected dial plan.	Read only, for information purposes only.
Template Name	Name of the selected template name.	Read only, for information purposes only.
Model Name	Name of the selected model name.	Read only, for information purposes only.
Pattern Name	Enter a name for the new pattern.	This is a mandatory field.
Description	Enter a description for the pattern.	Optional Field
Site Specific	Select this check-box if you would like this pattern to be specific to a particular site.	
Customer Specific	Select this check-box if you would like this pattern to be specific to a customer.	

Field	Description	Remarks
Site Type	Specify the site type relevant to this pattern.	
Transaction Type	Specify the transaction type relevant to this pattern. For example, AddLocation.	
ISO Country Code	Select the relevant ISO country code from the drop-down list.	The default for this value is None.
Date Added	Date that the pattern was initially added to the system.	Read only, for information purposes only.
Pattern Definition		
Translation Pattern	Enter the translation pattern, including numbers and wild cards. For example, "#NATCODE##FNN#".	Please do not use spaces in your translation patterns.
Partition	Select the required partition from the drop-down list.	If you do not want to assign a partition, select None.
Calling Search Space	Select the required call searching space from the drop-down list.	
Route Option	The Route Option indicates whether you want this translation pattern used for routing calls or for blocking calls. Select the required route option from the drop-down list.	
Provide Outside Dial Tone	Select this check-box if an external dial tone is required.	
Urgent Priority	Select this check-box if this pattern requires urgent priority.	Important: All supported versions of CCM currently set all translation patterns with a n urgent priority, this field cannot be changed.
Route Next Hop By Calling Party Number	Select this check-box to enable routing based on the calling party number.	
Use Originator's Calling Search Space	Select this check-box to make use of the <i>Use Originator's Calling Search Space</i> setting on translation pattern definitions (Unified CM 10.0 or later).	Default value is false.
Calling Party Transformations		
Use Calling Party's Phone Mask	Select this check-box if you would like the full, external phone number used for calling line ID (CLID) on outgoing calls.	
Calling Party Transform Mask	Enter a transformation mask value. If this field is left blank and the Discard Digits field is not checked, no calling party transformation takes place.	Valid entries include digits 0 to 9, the wild card character X. This field can also be left blank.

Field	Description	Remarks
Prefix Digits (Outgoing Calls)	Enter the required prefix digits. The appended prefix digit does not affect which directory numbers route to the assigned device.	Valid entries include digits 0 to 9, #, *. This field may also be left blank.
Calling Line Presentation Bit	Select the required option from the drop-down list, options include Default, Allowed and Restricted.	
Calling Name Presentation Bit	Select the required option from the drop-down list, options include Default, Allowed and Restricted.	
Called Party Transformations		
Discard Digits	A discard digits instruction (DDI) removes a portion of the dialled digit string before passing the number on to the adjacent system. Specify the discard digits instructions you want associated with this route pattern.	A DDI must remove portions of the digit string, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.
Called Party Transform Mask	Enter a transformation mask value. If this field is left blank, no calling party transformation takes place.	Valid entries include digits 0 to 9, the wild card character X. This field can also be left blank.
Prefix Digits (Outgoing Calls)	Enter the required prefix digits.	Valid entries include digits 0 to 9, #, *. This field may also be left blank.

Procedure

Managing Route Patterns

To manage route patterns within a particular model:

- Step 1** Browse to *Dial Plan Tools > Model Management*.
- Step 2** Select the *Manage Route Patterns* active text link.
- Step 3** Select the *Dial Plan* (active text link) to modify.
- Step 4** Select the *Template* (active text link) to modify.
- Step 5** Select the *Model* (active text link) to modify.

The resulting page will list all route patterns available for the selected dial plan, template and model. From this page you are able to add, modify, delete and apply route patterns.

Procedure

Deleting a Route Pattern

- To delete a route pattern, select the check-box adjacent to the relevant route patterns then click the **Delete Selected** button.

The route pattern will be removed from the dial plan.

Procedure

Modifying a Route Pattern

- To modify a route pattern, select the **name** (active text link) of the route pattern that you would like to modify, make the required modifications then click the **Modify** button.

The route pattern will be updated within the system.

Procedure**Adding a Route Pattern**

- To add a route pattern, select the **Add** button, complete all of the required fields, then click the **Add** button.

The route pattern will be added to the Dial Plan.

The following fields are available:

Field	Description	Remarks
Specific Information		
Dial Plan Name	Name of the selected dial plan.	Read only, for information purposes only.
Template Name	Name of the selected template name.	Read only, for information purposes only.
Model Name	Name of the selected model name.	Read only, for information purposes only.
Pattern Name	Enter a name for the new pattern.	This is a mandatory field.
Description	Enter a description for the pattern.	Optional Field.
Customer Specific	Select this check-box if you would like this pattern to be specific to a customer.	
Transaction Type	Specify the transaction type relevant to this pattern. For example, <i>AddLocation</i>	
ISO Country Code	Select the relevant ISO country code from the drop-down list.	The default for this value is <i>(None)</i> .
Release Cause	Specify the release cause code to be used for this route.	
Route List Name	Specify the route list name for the route. For example, VOICEMAIL.	
Destination Type	Specify the destination type for the route.	
Enable CMC	Select the check-box to enable Client Matter Codes.	
Date Added	Date that the pattern was initially added to the system.	Read only, for information purposes only.
Pattern Definition		
Translation Pattern	Enter the route pattern, including numbers and wild cards For example, <i>"#NATCODE##FNN#"</i> .	Please do not use spaces in your route patterns.
Partition	Select the required partition from the drop-down list.	If you do not want to assign a partition, select <i>None</i> .

Field	Description	Remarks
Route Option	The Route Option indicates whether you want this route pattern used for routing calls or for blocking calls. Select the required route option from the drop-down list.	
Provide Outside Dial Tone	Select this check-box if an external dial tone is required.	
Urgent Priority	Select this check-box if this pattern requires urgent priority.	Important: All supported versions of CCM currently set all route patterns with an urgent priority, this field cannot be changed.
Require Forced Authorization Code	Select this check-box if this pattern requires the use of a Forced Authorization Code.	
Authorization Level		
Calling Party Transformations		
Use Calling Party's Phone Mask	Select this check-box if you would like the full, external phone number used for calling line ID (CLID) on outgoing calls.	
Calling Party Transform Mask	Enter a transformation mask value. If this field is left blank and the <i>Discard Digits</i> field is not checked, no calling party transformation takes place.	Valid entries include digits 0 to 9, the wild card character X. This field can also be left blank.
Prefix Digits (Outgoing Calls)	Enter the required prefix digits. The appended prefix digit does not affect which directory numbers route to the assigned device.	Valid entries include digits 0 to 9, #, *. This field may also be left blank.
Calling Line Presentation Bit	Select the required option from the drop-down list, options include Default, Allowed and Restricted.	
Calling Name Presentation Bit	Select the required option from the drop-down list, options include Default, Allowed and Restricted.	
Called Party Transformations		
Discard Digits	A discard digits instruction (DDI) removes a portion of the dialled digit string before passing the number on to the adjacent system. Specify the discard digits instructions you want associated with this route pattern.	A DDI must remove portions of the digit string, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.
Called Party Transform Mask	Enter a transformation mask value. If this field is left blank, no calling party transformation takes place.	Valid entries include digits 0 to 9, the wild card character X. This field can also be left blank.

Field	Description	Remarks
Prefix Digits (Outgoing Calls)	Enter the required prefix digits.	Valid entries include digits 0 to 9, #, *. This field may also be left blank.

iFINT Migrate Feature

The iFINT migrate feature allows a system administrator to update the format of IPPBX configured FINTs on the Cisco Unified Communications Manager (Unified CM) when changes to the current dial plan number construction settings in the system have been made.

The updates to the Unified CM will be made specifically to *Directory Numbers or Patterns (dnorpatterns)* that belong to the following pattern usage groups:

- Device
- Call Pick Up Group
- Hunt Pilot
- Directed Call Park

Number Construction Rules

The format of IPPBX Configured Internal Numbers can be changed under the *Dial Plan Tools > Number Construction* section in the system. iFINT Number construction settings currently supported are grouped under the heading *Format of IPPBX Configured Internal Number* and include:

- Includes CID
- Includes CPID
- Includes RID
- Includes SiteCode
- Includes Extension

Activating the iFINT Migrate Functionality

Once the dial plan's number construction settings for iFINTS have been set, the numbers on the Unified CM can be updated using the system's *Model Migration* tool.

Procedure

To migrate all affected iFINTs at specific locations:

- Step 1** While logged in as a System level user, browse to *Dial Plan Tools > Migrate Models*.
- Step 2** Use the hierarchy filters at the top of the page to filter the number of locations displayed. Select one or more locations for iFINT migration and click the **Migrate Selected** button to start the process.
- Step 3** **Enable** the migration option *IPPBX Configured Internal Number Migration* and click **Next**.
- Step 4** Click the **Start Migration** button to start the process

The iFINT migration will now be applied to numbers at all selected locations.

iFINT Migration History Logs

The system keeps a detailed log of all migrations that have been applied at any location.

Procedure

To view iFINT migration history logs:

- Step 1** While logged in as a System level user, browse to *Dial Plan Tools > Migrate Models* .
 - Step 2** Use the hierarchy filters at the top of the page to filter the number of locations displayed.
 - Step 3** Click the **History** button next to any location in the list to display the location's migration history log.
-

Dial Plan Terms

See below for a list and description of dial plan terms:

- **CPID:** This is the Call Processing ID. This is assigned to hardware as required (e.g. PBX, PGW, Voicemail, etc.). The CPID is generally configurable when adding the hardware and is displayed when viewing the settings.
- **RID:** Routing ID. This is configurable as to whether it is a customer level or location level ID. Although it is configurable, if anything other than Location is selected you will likely have problems. This ID is selected for a location and is unique for the CPID. In the case of a location, the RID could be an available rid for the CPID of the IPPBX of the location. The RID assigned to a location can be viewed on the location details page under the dial plan section (if enabled).
- **Site Code:** This is a location level code assigned for each location. In the system, this would be required if you wanted more than a single location in the system (as the fint needs to be unique). The site code inventory is managed per customer in the system. The length of the site code is always allowed to be variable with a defined maximum length. Overlapping site codes are not allowed within a customer - if a site code of 1 was defined, then a site code of 12 would not be allowed. The site code for a location can be viewed on the location details screen under the Dial Plan section.

Note

The above description relates to the G1 dial plan. In the G2 dial plan, the number construction for the FINT (the DNs provisioned on phone lines in Unified CM) will not include the site code. However, when creating FINTs in CUCDM, the CUCDM will still use site codes as per G2 number construction rules. Therefore when the administrator is configuring customers/ locations in G2, site codes are still required by CUCDM to keep numbers unique within CUCDM. The G3 dial plan is based on the HCS-G2 dial plan model and assumes that the SMB's have a flat dial plan with EXT-only DNs. The fundamental difference between the HCS-G2 and HCS-G3 dial plan is that HCS-G3 adds customer-specific site partitions and CSSs at the AddCustomerHardwareGroup step, and then these settings are used by the phone partitions and CSSs to ensure that each customer can have independent calling partitions, and can overlap DN numbers.

- **CID:** Cluster ID. This is an ID assigned to each Cisco Unified Communications Manager PBX cluster in the system. This is configurable when adding the cluster and can be viewed on the cluster details page.
- **Fint:** The full internal number the system knows the lines as. The construct of this is defined in the number construction rules. When a location is added, the full fint inventory is created for the location.

- FNN: The full national number (PSTN number).

Number Construction

Caution

The number construction settings configured upon initial installation must only be changed by a suitably qualified person who has an in-depth knowledge of dial plan rules and number construction, and who is fully aware of the possible consequences of making such changes. Incorrect settings will lead to inconsistent dial plan behavior, which may result in erratic call flows and faulty call connections.

Dial Plan guide (used in conjunction with the Number Construction Screen on the system GUI). This is accessed from *Dialplan Tools > Number Construction*.

Details

This is a place to give the Dial Plan a name and description.

Codec Selection

These are the codecs used by the system when setting up the per location Cisco Unified Communications Manager regions for locations.

Dial Plan Rules

Multi-Tenant Dial Plan?: This setting is used to determine certain behavior within the system and should be enabled.

Enforce HCS Dial Plan?: This setting determines the behavior in a few places in the code which allows the flexibility of working around certain validations put in place for HCS. This is currently:

- When a hardware group is associated/disassociated with a customer in a HCS dial plan, the provisioning of devices in the hardware group will occur. This includes PBXs and PGWs.
- When enabled, the requirement for the hardware group from addCustomer is removed. This enables the assignment of hardware groups to customer after they are created. Since there is no hardware for AddCustomer, there are no hardware transactions during this transaction (ie PGW or IPPBX).
- The Customer Advanced Mgt. page is altered with this setting enabled. The View PGW Config button is hidden and the Hardware group Association button is visible.
- The customer will be able to manage which hardware groups are available to the locations. Only hardware groups that are listed under the Allowed Hardware groups section of the Customer Hardware group Management page will be accessible to the locations. If no hardware groups are associated, AddLocation will not be possible. Customer Administrators can access the Customer Hardware group Management page by browsing to General Administration > Customers > <Customer Name> > Advanced Mgt. > Hardware group Association.
- At the location level, when adding a location only the hardware groups that have been associated with the customer are available. This is also true for other places in a customer where hardware group options are available (e.g. Voicemail, AA, etc).

Site Type Selection: You can turn on support for site types; then select the site types you need. Site types are selected when you add a location and the site type is appended to the end of model names for location transactions (e.g. RegisterPhone-Office).

Internal Number Format

This is used to determine the format of the internal numbers (fints) in the system and the length. The fint is the way the number is stored internally inside the system. The fint currently needs to be unique in the system. If, for example, you select only the *Includes Site Code* checkbox, then you cannot have the same site code in more than one customer (as the fint would be SiteCode + Extension only).

Note

If you change these settings, it will NOT affect any fints already in the system. It will affect any new fints added to the system (i.e. locations). However, changing this after you've added customers and locations will likely lead to errors and failed transactions. This needs to be correct before you start deployment.

Available fields include:

- **Internal Number Component Order:** Used to specify the order of number components. This field cannot be edited and is included for information purposes only. For example CPID:RID:SITEPREFIX:CID:SITECODE:EXTNTYPE:EXTNNUMBER.
- **Maximum Allowed Internal Number Length:** This is the maximum allowed fint length. Default is 20 characters. This cannot be less than the total allocated digits and the internal fint digit length cannot be greater than the max allowed length.
- **Includes CPID?:** Select this checkbox if you want the CPID to be included in the fint. Regardless of whether this is selected or not, CPIDs are still assigned to most devices, including PBXs, Transits, Gateways, Voicemail, etc.
- **CPID Digits:** The number of digits to use for the CPID. As the CPID is still allocated for hardware even if it's not being used in the fint, this should be set to a sensible number depending on the number of hardware devices being planned (i.e. at least 2 digits).
- **Includes RID?:** Select this checkbox if you want the RID to be included in the fint. Regardless of whether you select this or not, RIDs are still allocated to Locations/Customers.
- **RID Digits:** The number of digits to use for the RID. As RIDs are still allocated to locations even if it's not being used in the fint, this should be set to a sensible number depending on the number of locations/customers being planned (i.e. at least 3 digits).
- **Includes CID?:** Select this checkbox if you want the CID to be included in the fint. Regardless of whether you select this or not, CIDs are still allocated to Cisco Unified Communications Manager (Unified CM) PBX clusters.
- **CID Digits:** The number of digits to use for the CID. As CIDs are still allocated to Unified CM PBXs even if it's not being used in the fint, this should be set to a sensible number depending on the number of clusters being planned.
- **Includes Site Code?:** Select this checkbox if you want the site code to be included in the fint. Regardless of whether you select this or not, Site Codes are still required for locations to be added.
- **Max. Site Code Digits:** This is a number to reflect the maximum number length of the site code.
- **Site Code Rules:** Free text which is displayed next to site codes when they are being added to the system to communicate the rules imposed by the dial plan. This should be useful to the user: e.g. 'Maximum length of 4 digits'.
- **Variable Length Internal Number?:** Select this checkbox if you want the length of the extension portion of the fint to be configurable. If Variable Length Internal Number is set to Y, the Internal Number Length field must be blank. Enabling this will result in an extension length setting

being available during add location. This enables administrators to define the length of the extensions. If this is not selected, the length of the extension is determined by taking the setting below and subtracting any other digits from it (i.e. a location has a site code of 123 (3digits) and the dialplan calls for no CPID, no RID, and 7 for internal number length. This would result in the extension length being $4 = 7 - 3$.

- **Internal Number Length:** This allows the user to define the length of the internal number. This is used only if the variable length extension is not enabled. See the note above to determine the extension length.

Internal Number Display Rules

This setting determines how internal numbers are displayed within the application. This drives a value `displayfintnumber` which is used anytime the fint would be displayed to the user (within the GUI, self care, default line text in Cisco Unified Communications Manager, etc.).

Note

If you change this setting, it will NOT affect any fints already in the system. It will affect any new fints added to the system (i.e. locations).

- *Includes CPID?:* Selecting this checkbox will include the CPID in the number display.
- *Includes RID?:* Selecting this checkbox will include the RID in the number display.
- *Includes Site Code?:* Selecting this checkbox will include the Site Code in the number display.

RID Type Selection

This setting determines the hierarchy the RID is allocated for. See the RID notes above: only location is fully supported today and is the only option that should be selected.

Dial Prefixes

This section covers any dial prefixes that are required for various call types. This allows the requirements to be turned on/off as well as specification of the value.

- *Inter-Site Prefix Required?:* This setting determines if an inter site prefix is required for the dial plan.
- *Inter-Site Prefix Configurable?:* This setting determines if the prefix is a configurable value. This is configurable per customer and can be defined for the customer when adding. If configurable is not enabled, then the value used during `AddCustomer` is hard-coded to 8.
- *PSTN Access Prefix Required?:* This setting determines if a PSTN breakout code is required.
- *PSTN Access Prefix Configurable?:* This setting determines if the prefix is a configurable value. This is configurable per location and can be defined for the location when adding. If configurable is disabled, then the value used during `AddLocation` is hard-coded to 9.
- *Call Park Prefix?:* To distinguish between Call Park numbers internally, the system uses a custom prefix, followed by a number increment, one per call processing server in a Location's Cisco Unified Communications Manager group. For example, if an administrator selects #2 as a Call Park Prefix and creates a 10 number Call Park range, the numbers would be #20110, #20111 etc. on Server A and #20200, #20201 etc. on Server B.
- *Call Park Location Configurable?:* This setting determines if the prefix is a configurable value. If checked, the value in the Call Park Prefix field will be displayed at a location level in a read-only text field. This will then be configurable per location and can be defined for the location

when adding. If configurable is disabled, then the value used during the Add Location operation is hard-coded.

Format of External Phone Number Mask on Unified CM

This section determines how external (E164/FNN) numbers are displayed in the system. This includes in drop-downs for assigning lines to phones/users and also for configuring the external mask in Cisco Unified Communications Manager for the lines.

Note

If you change this setting, it will NOT affect any FNNs already in the system. The *displayed 164* value is determined for the number when it is added to the system's e614 inventory. It will affect any new FNNs added to the system.

- Show PSTN Dial Prefix: This will include the PSTN breakout prefix on the front of the number.
- Show Country Code: This will include the country code at the beginning of the number (i.e. 44 for the UK).
- Show National Code Prefix: This will display any trunk access code on the front of the PSTN number (i.e. 0 for the UK).
- Show National Code: This will display any area code on the front of the PSTN number.

Format of IPPBX Configured Internal Number

This section determines how the FINT numbers are provisioned in the IPPBX system (the DN in CallManager). This is generally done when you setup a device with an extension number (phones, user mobility, CTI, etc.). This also affects any features that make use of the FINTs (e.g. Pickup Groups, Hunt Groups, SNR, etc.). The full list of features that uses the iFint logic is:

- Phone Lines configuration
- Roaming Profile (Device Profile) lines
- CTI route points/ port lines
- Analog Port Lines
- Pick up Groups - number and members
- Number Group (line group in Cisco Unified Communications Manager) members
- Hunt Group Pilot numbers
- Location Call Park Numbers
- SNR Setup (Remote Destinations, etc.)

Note

If you change this setting, it will not affect any FINTs already provisioned in the system. It will only affect any new FINTs added to the system. Changes can however be applied to existing locations using the iFint Migrate feature; see [iFINT Migrate Feature on page 549](#) for more details on this tool.

The following options are available to setup the number configured into the IPPBX:

- Includes CID

- Includes CPID
- Includes RID
- Includes SiteCode
- Includes Extension

The default setting for the *Includes SiteCode* and *Includes Extension* checkbox is *Selected (ON)* .

Format of Voicemail Configured Pilot Number

This section determines how the Voicemail pilot numbers are provisioned in the IPPBX system (the DN in CallManager). The default setting for the *Includes Inter-site Prefix* checkbox is *Not Selected (OFF)* . The default setting for both the *Includes SiteCode* and the *Includes Extension* checkbox is *Selected (ON)* .

Note

- These default settings are critical to ensure backward compatibility when a customer updates to a later software version. If you change these default settings, the Voicemail feature for your location will not function.
 - However, if a customer is using **only** the extension number in their existing system configuration, the *Includes SiteCode* checkbox must be **unselected** (switched off) after upgrading to a later software version.
-

The following fields/options are available:

- Includes Inter-Site Prefix. Selecting this checkbox will result in the inter-site prefix being included in the Voicemail pilot number.
- Includes SiteCode . Selecting this option will include the site code in the Voicemail pilot number.
- Includes Extension. Selecting this option to include the extension in the Voicemail pilot number.

Format of Voicemail Configured Mailbox Number

This section determines how Voicemail mailbox numbers are provisioned in the IPPBX system (the DN in CallManager). The default setting for both the *Includes SiteCode* and the *Includes Extension* checkbox is *Selected (ON)* .

Note

- These default settings are critical to ensure backward compatibility when a customer updates to a later software version. If you change these default settings, the Voicemail feature for your location will not function.
 - However, if a customer is using **only** the extension number in their existing system configuration, the *Includes SiteCode* checkbox must be **unselected** (switched off) after upgrading to a later software version.
-

The following fields/options are available:

- Includes SiteCode. Selecting this option will include the site code in the Voicemail mailbox number.

- Includes Extension. Selecting this option will include the extension in the Voicemail mailbox number.

Configurable FINTs

The functionality allows a subset of Full Internal Numbers (FINTs) to be provisioned as Directory Numbers on the Cisco Unified Communications Manager (Unified CM) instead of the complete FINT.

The Configurable FINTs can be comprised of CPIDs, Routing ID's (RIDs), Cluster ID (CID), Site Location Code (SLC) and Extension Number. The format of Configurable FINTs can be defined from the Number Construction Rules. All the phone lines, mobility lines, CTI route points/ port lines, analog port lines, pick up group numbers, pickup lines, line group members, hunt group pilot numbers, call park numbers will be provisioned as configurable FINT number on the Unified CM.

Number Construction Rules

Configurable FINTs are defined by browsing to *Dialplan Tools > Number Construction* . The following options are available under the section *Format of IPPBX Configured Internal Number* on the *Dialplan Management* screens to define the format of the Configurable FINTs:

- Includes CID
- Includes CPID
- Includes RID
- Includes SiteCode
- Includes Extension

Note

By default, the settings for *Includes SiteCode* and *Includes Extension* are set to true.

Loading Configurable FINTs rules

The following columns are used to load the Configurable FINTs rules:

- IPPBX Configured FINT has CPID
- IPPBX Configured FINT has RID
- IPPBX Configured FINT has CID
- IPPBX Configured FINT has Site Code
- IPPBX Configured FINT has Extension

The columns take the values true or false. By default the value of *IPPBX Configured FINT has Site Code* and *IPPBX Configured FINT has Extension* are set to true.

Recommended Dial Plan Configuration by Solution

HCS Solution

The recommended setup for a HCS deployment is outlined below:

Note

Any setting not mentioned below can be configured as required for the deployment.

Dial Plan Rules

The following settings are required:

- Multi-Tenant Dial Plan: This should be enabled
- Enforce HCS Dial Plan: This should be enabled

Internal Number Format

As the fnt needs to be unique in the system, Site Code and Extension only cannot be used unless customers will not use the same site codes. The recommendation is to use the CPID as this will allow a prefix which will only be used internally by the system to make the number unique. The first digit of the site code should be the intersite prefix for the solution and need to match the configured intersite prefix for the customer.

The following settings are required:

- Includes CPID: This should be enabled
- CPID digits: Depends on the number of devices expected, but recommend 3 digits minimum
- Includes RID: Optional - should be enabled if overlapping site codes on the same cluster are expected.
- RID digits: Depends on the number of locations expected, recommend 3 digits minimum
- Includes CID: This should be disabled
- CID digits: Not required as CID is disabled
- Includes Site Code: This should be enabled.
- Max site Code length: This depends on the dial plan being deployed
- Site Code Rules: Adjust this field to reflect the max length configured
- Variable Length internal number: This can be set as needed depending on the dial plan
- Internal Number length: This can be set as needed depending on the dial plan
- RID Type selection: This should be set to Location

Note

When using a HCS dial plan, numbers are constructed using SLC + Extension (ISP is assumed in the site code). However, this means that if two separate customers use the same extension in locations with the same site code, a conflict can occur as fnts from the two customers may match. To avoid this scenario, it is important to ensure that the *Includes CPID?* checkbox is selected. This will ensure that two separate HCS based customers never have fnts that match. It is important to ensure that this option is selected before deploying phones as changing this option post-deployment can lead to complications with the dial plan. If the solution is expected to support multiple customers using the same

site code on the same IPPBX, then the *Includes RID?* checkbox should also be enabled.

Dial Prefixed

The following settings are required:

- **Inter-Site Prefix Required:** This setting can be either way. However recommendation is that the setting is off and any use of that variable is replaced in the model with the actual value (e.g. 8 instead of #ISP#). The only affected part of the Unified CM model in the HCS sample dial plan is the translation patterns for Intrasite calls where the ISP is included in the pattern (so replaced with an 8 instead). This value might need to be updated if the deployment uses a different value for ISP. This will ensure that the ISP is not visible or configurable in the system. If the intersite prefix variable is required in any models (e.g. #ISP# in the Unified CM model) or it varies by customer then this will need to be enabled for the variable to be replaced correctly.
- **Inter-Site Prefix Configurable:** The intersite prefix needs to match the first digit of the site code, so the default value in the system if this is disabled is 8. If that is acceptable then this setting can be off. If it needs to be a different value then this should be enabled so an appropriate setting can be determined for the customer.
- **PSTN Access Prefix Required:** This depends on the dial plan, but typically it is on.
- **PSTN Access Prefix Configurable:** Either can be selected, depends on the design requirement.

Format of IPPBX Configured Internal Number

With HCS the dial plan design is based on SiteCode + Extension being in the Unified CM so it should be set to:

- Includes SiteCode
- Includes Extension

Device Pool Templates

Device pool templates are created by Provider Administrators and can be used by Customer and lower level Administrators. Device pool templates are used to specify a pre-defined set of settings/options to be used when creating new device pools. Once a device pool has been created using a template, no reference remains between the template and the device pool. Any changes made to the device pool do not affect the device pool template used to create the device pool, and similarly any changes made to the device pool template do not affect any device pools created using that device pool template.

The device pools are in turn applied to devices such as phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, CTI route points, CTI ports, Remote Destination Profiles, and so on, where they indicate certain key device features, which include:

- CCM Group
- Date/Time Group
- Audio Regions
- Local Route Group
- AAR Calling Search Space
- AAR Group

- Calling Party Transformation CSS
- Called Party Transformation CSS
- SRST Reference

Device pool templates are used to make common resources and settings available to devices that make use of device pools created using that device pool template. In most cases the Provider Administrator can choose between "Typical"/"None" behavior and custom values. This allows the Provider Administrator to create a structure for Customer Administrators to create device pools at the Location level.

The *Device Pool Templates* screen displays all currently configured device pool templates.

Existing device pool templates can be modified by selecting the relevant device pool template *Name* (active text link).

New device pool templates can be created by clicking the **Add** button.

A search facility is available to search for a specific template by entering the relevant search criteria, and then clicking the **Search** button.

Existing device pool templates can be deleted by clicking the **Delete** button adjacent to the relevant device pool template name.

Multiple device pool templates can be selected and deleted (if required) by selecting the appropriate checkboxes and/or clicking the relevant **Select All**, **Select None**, and **Delete Selected** buttons.

Typical Device Pool Template Configuration

To effectively configure device pool templates complete the following:

1. Import the Date/Time Groups CCM item from Unified CM to make sure that the correct date/time groups are in the system. See [Importing/Refreshing CCM Items on page 87](#) for details.
2. Configure (add) the required device pool templates. See [Adding a Device Pool Template on page 559](#) for details).
3. Add an SRST role to the IOS device (if an SRST reference is required). See [SRST Role on page 355](#) for details.

Adding a Device Pool Template

Device pool templates, created at the PBX level, are used as templates for any new device pools that are created. Fields have a radio button each with a choice of "Typical" (previous behavior, automatically set by system) "None," or a dropdown with a list of appropriate values. For certain settings that are Location specific, the template values can be set to "Choose at Device Pool Level," which means that the value is included in a drop-down on the device pool screen during creation and editing.

Procedure

To add a device pool template:

- Step 1** Click the **Add** button on the *Device Pool Templates* screen.
- Step 2** Complete all the required fields, and then click the **Add** button.

Available device pool template fields include:

Field	Description	Remarks
Device Pool Template Name	The name for the device pool template.	This is a mandatory field.
Description	A brief description of this device pool template.	-
CCM Group	The CCM group to associate with this device pool template. Available radio buttons are: <i>Typical</i> , which sets the Cisco Unified Communication Manager (Unified CM) Group to whichever Unified CM group has the lowest load when adding the device pool at location level. When adding subsequent device pools to the location, <i>Typical</i> uses the Unified CM group that was selected when the Location was initially created; or <i>Select from Drop Down</i> , which allows the Administrator user to specify a Unified CM Group to use; this selection appears in the drop-down list as the chosen value when adding the device pool.	Select the required radio button.
Date/Time Group	The date/time group required. Available radio buttons are: <i>Typical</i> , which sets the date/time group to the same value as the Locations time zone. To ensure this works as expected, the Date/Time groups used in Unified CM must conform to the naming convention used in CUCDM; or <i>Select from Drop Down</i> , which allows the Admin user to specify the date/time Group to use; this selection appear in the drop-down as the chosen value when adding the device pool.	Select the required radio button.
Audio Regions	<p>The audio regions required. Available radio buttons are: <i>Typical</i>, which uses the Legacy Codec Region for the Location, this depends on whether Location, Customer or Dial Plan Codecs are applied at the Location. When the device pool is added this value is set to 'Use Codec Default'; or <i>Select from Drop Down</i>, which allows the Admin user to specify the required audio region.</p> <p>This default region is dependent on where the chosen bit rates have been configured. Options include Location level bit rates, Customer level bit rates, and Dial Plan level bit rates. For details around how and where these bit rates can be configured, see: Operations Tools on page 950.</p> <p>The audio regions available in this drop-down list are those created via Network > PBX Devices - see Adding an Audio Region on page 648 if required.</p>	Select the required radio button.

Field	Description	Remarks
Local Route Group	<p>The Local Route Group (LRG) required. Available options are: <i>None</i> - sets this value to None when adding a device pool; <i>Use Location LBO</i> (LBO, or Local Break Out is the term used to describe a scenario where devices are configured to break out to the PSTN through a gateway device at the same location) - if a Location LBO exists then the LRG is looked up and shown as read-only when adding the device pool. If no LBO exists then this value is set to <i>None</i>. The Administrator user can modify this on the device pool at a later stage. This option is offered to make adding additional device pools easier, by looking up the LBO; or <i>Allow text entry at Location level</i> - when adding the device pool the LRG has a text box allowing the Administrator user to specify the route group to use.</p> <p>This option is offered, since not all route groups are managed in CUCDM, and may not exist at the time of creating the device pool. This is a textbox, as opposed to a dropdown, since the LRG will not exist at the time of creating the Location. This allows the user to specify a route group once it has been created. If during add location a value is specified that does not exist in Unified CM, the operation fails. The value is validated when modifying the device pool, but again, since not all route groups are managed in CUCDM, this value is entered as free text.</p>	Select the required option from the drop-down list.
AAR Calling Search Space	The AAR calling search space required. Available radio buttons are: <i>None</i> - sets this value to None when adding a device pool (non-editable); or <i>Use Global Setting</i> - sets the value as provisioned by the Model.	Select the required radio button.
AAR Group	The AAR group to associate with the device pool template. Available radio buttons are: <i>None</i> - sets this value to None when adding a device pool (non-editable), or <i>Use Global Setting</i> - sets the value as provisioned by the Model.	Select the required radio button.
Calling Party Transformation CSS	Available radio buttons are: <i>None</i> - sets this value to None when adding a device pool (non-editable), or <i>Use Global Setting</i> - sets the value as provisioned by the Model.	Select the required radio button.
Called Party Transformation CSS	Available radio buttons are: <i>None</i> - sets this value to None when adding a device pool (non-editable), or <i>Use Global Setting</i> - sets the value as provisioned by the Model.	Select the required radio button.

Modifying a Device Pool Template

Procedure

To modify a device pool template:

- Step 1** Select the required device pool template *Name* (active text link) that you want to modify on the *Device Pool Templates* screen.

- Step 2** Update the required fields, and then click the **Modify** button. Refer to the table under [Adding a Device Pool Template on page 559](#) for details on each field if required.

Note

The displayed device pool template can also be deleted by clicking the **Delete** button on this screen.

Feature Configuration Templates

The Feature Configuration Template (FCT) feature is a mechanism to allow call routing settings, such as Route List and CSS, to be configurable when adding or modifying specific system features, e.g. Number Translations, without exposing them on the GUI. The reason for using templates is that a customer or location administrator does not necessarily understand the complicated call routing concepts.

FCTs consist of various FCT elements. Each FCT element represents a particular call routing model, e.g. Route Patterns and/or Translation Patterns.

- There are no limits on the number of FCTs the user can create. The templates are added at Customer level and can only be added/viewed/deleted by Customer admin and higher level roles. The FCT feature is in other words meant as a generic solution for multiple features, e.g. Number Translations.

Adding Feature Configuration Templates

- Feature Configuration Templates can only be added by using bulk loaders. The *Add Feature Config Template* worksheet (available in the *Resources* sample workbook) contains the following relevant columns: *Feature Configuration Template Name*, *Feature Parameters 1*, *Feature Parameters 2*, etc.
- Feature Configuration Template Elements can be added by using the *Add Route Pattern Element* and *Add Translate Pattern Element* worksheets.
- For more information on bulk loading, please see the *Bulk Loader Guide*.

Note

Feature Configuration Templates cannot be modified.

Procedure

Deleting Feature Configuration Templates

To delete a Feature Configuration Template (FCT):

- Step 1** Browse to *General Administration > Configuration Templates*.
- Step 2** Select the checkboxes associated with the *Template Names* to delete. (By clicking on the *Select All* active text link at the bottom of the screen, all the checkboxes will be selected at once.)
- Step 3** Click the **Delete Selected** button.

Note

Once a feature is associated with a FCT, the FCT cannot be deleted until the feature is disassociated from the FCT.

Procedure

Deleting Feature Configuration Template Elements

To delete a Feature Configuration Template Element:

- Step 1** Browse to *General Administration > Configuration Templates*.
 - Step 2** Select the *Template Name* (active text link).
 - Step 3** Select the *Element Name* (active text link).
 - Step 4** Click the **Delete** button.
-

Note

Once a feature is associated with a FCT, the elements of the FCT cannot be deleted until the feature is disassociated from the FCT.

End User Migration

The *End User Migration* screen enables a customer administrator to migrate (move) users from one location to another or a reseller administrator to move users from one building to another. In each case, the users' phone/s and services are also migrated.

After the users have been selected and moved on this screen, details can be previewed, and a bulk loader sheet containing all the relevant information is generated. This sheet can then be reviewed, and bulk loaded using the standard bulk loader functionality.

Note

Migrations can only take place between locations or between buildings and not from a location to a building or building to location.

Procedure

To migrate end users:

- Step 1** In the *Source* column, the end users that you want to migrate (move) are shown by selecting their current *Building*, *Customer*, *Division* and *Location* from the respective drop-down lists. The items available for selection depend on the item selected from the parent list, so that for example only locations that belong to a particular division are shown.

The end users that meet the selection criteria are displayed in the *End Users* list. The *End Users* list can be filtered further by selecting search criteria, for example *Username starts with* or *Username ends with* on the *Search* drop-down list and entering search criteria in the input box.
- Step 2** In the *Destination* column, select the *Building*, *Customer*, *Division* and *Location* where the users are to be migrated.
- Step 3** Select users to migrate from the *End Users* list to the *Migrating* list and select the **Add >>** or **All >>** button as required.

Manage the users to migrate by selecting them and moving them with the **Add >>**, **All >>**, **<< Remove**, **<< All** buttons and the *Select All* links above the lists.

An error pop-up message displays if invalid selections or actions are made.

- Step 4** When the *Destination* column entries are completed, click the **Preview Migration** button to display the details of the phones and services that will be migrated, and to complete the user migration and generate the bulk loader sheet.
-

Caveats

Take note of the following caveats when migrating end users:

- Admin users can **not** be migrated, and are therefore not available for selection in the drop-down list.
- End user migration is limited to within the same PBX - cross PBX end user migration is not supported.
- Excluding building locations, end users can only be migrated within the same customer. Buildings locations end users can be migrated between PBX's provided that the Customers are using shared hardware.
- Conference server 'Webex' will not be migrated, but will be removed from the user when migrated. a Webex side-issue prevents immediate re-provisioning of an end user with the same email address.
- Migrating end users to a location that does not use the same Cisco Unity Connection Voicemail service is not supported.
- Phone types with the *Owner Username Required* field enabled will not be migrated.
- No validation exists to prevent migrating devices to an SRST device pool that will result in the SRST device becoming over-subscribed.
- End User services are not added or removed as part of the end user migration - the source and target locations must support all of the services specified as part of the migration (specifically conferencing and voicemail).
- When migrating an LDAP authentication end user, the target location must be enabled for LDAP authentication, or the migration will fail.
- Busy lamp fields, phone services and service URL's associated to lines being migrated are removed and not re-added at the target. Only speed dials will be successfully migrated.
- If altering line mappings as part of the migration, any migrated cloned lines created at the target location as part of the migration could result in unexpected failures depending on the line ordering.
- Migrating extensions associated to FNNs are blocked when in use by users being migrated, but can be specified at the target location.
- Netwise and UC Central lines/users are explicitly excluded from migrations. Any such configurations must be removed before the end user is migrated.
- Lines belonging to line groups or pickup groups are removed from those groups. New line/call pickup groups are not created at the target location, and migrating lines are not provisioned within existing Line/call pickup groups. All groups will need to be provisioned after the migration is completed.
- Rollback scenarios for number groups (line groups) and call pickup groups will append the line to the end of the ordered list, not re-apply the line ordering from pre-migration.

End User Migration Preview

The *End User Migration* preview screen displays *From* and *To* columns containing the phones and services of the users to be migrated. This screen shows the result of the selections made on the [End User Migration on page 563](#) screen.

The entries in the *From* column are grouped by shared services and individual user lines. These include Device Pools, Voicemail Profiles, Conference Services, Subnets, Feature Groups, as well as individual end user Device Lines.

The entries in the *To* column show where each entry will be moved to at the migration target destination hierarchy. Edit the target destination if required by selecting a new target from the relevant drop-down list in the *To* column.

Note

If an error is detected in the end user migration, a message is displayed in bold text at the bottom-left of the screen, for example "No Voicemail Profiles available at target", and the **Generate Loader** button is not available. Resolve the error, for example, by creating a voicemail profile at the target destination, and then perform the end user migration again.

Once you are satisfied with the results/selections on this screen then click the **Generate Loader** button to generate a bulk loader sheet that can be saved and scheduled to load using the standard bulk loader functionality as described in the Bulk Loader Guide.

See also: [End User Migration on page 563](#).

Number Translations

An administrator can configure specific number translations to be applied to the dial plan. These translations are applied on either a Customer or Location level and are provisioned on Cisco Unified Communications Manager (Unified CM), PGW x10 or both (depending on administrator decision).

The number translations can be configured via the system's admin GUI, the bulk loaders or web service APIs.

Procedure

Viewing Number Translations

To view the Number Translations for a specific Customer or Location:

- Step 1** Browse to *General Administration > Number Translation*.
- Step 2** For a Customer administrator all the number translations for the relevant Customer and all its Locations are displayed. For a Location administrator only the number translations for that location are displayed.

The number of records displayed is dependent on the number selected in the *Max results* drop-down list - 10, 50 (default), 100, 500 or Unlimited. Click the **Next** button (if relevant) to view the next set of records. When there are no more records to display, the **Next** button does not function.

Procedure

Adding Number Translations

To add Number Translations for a specific Customer or Location:

- Step 1** Browse to *General Administration > Number Translation*.
- Step 2** Click the **Add** button.
- Step 3** Complete all the required fields. The following fields are available:

Field	Notes	Remarks
Pre-translated Number	The number on which Number Translation is applied.	There are no character-set limitations on pre-translated and post-translated numbers.
Post-translated Number	The number after the Number Translation has been applied.	There are no character-set limitations on pre-translated and post-translated numbers.
Target	An indication of which entities to apply the Number Translation to.	<p>Selection options in the drop-down list:</p> <ul style="list-style-type: none"> • Customer: This option provision Customer scoped Number Translations to each Cisco Unified Communications Manager (Unified CM) and/or PGW used by the customer. • Location: This option provisions Location scoped Number Translation only to the associated Unified CM. • All Locations: This option provisions the Number Translations for each location belonging to the Customer.

Field	Notes	Remarks
Feature Configuration Template	<p>The Feature Configuration Template and its associated elements (e.g. Route Patterns and Translation Patterns) used by the Number Translation.</p> <p>The selected Feature Configuration Template also determines the necessary models to use for the various number translation related transactions.</p>	<p>The list of available Feature Configuration Templates displayed in the drop-down is based on the selected <i>Target</i> (see above).</p> <p>If <i>Customer</i> is selected as a target, then only Customer-targeted templates are available.</p> <p>If a specific <i>location</i> is selected, then only templates targeted for that location type, that is Standard, Linked Child Site, Unmanaged or Shared Building locations) are available.</p> <p>If the <i>All Locations</i> target is selected, then all location-targeted templates are available; however, the template is applied to all locations of the template's type (e.g. to all Standard locations).</p> <p>For Number Translations it is possible to include both a Route- and Translation Pattern element to a template, but this would not be a typical use case. When adding a Number Translation a template should contain a Route Pattern element when the user wants to provision a Route Pattern on Cisco Unified Communications Manager (Unified CM) or a Translation Pattern element when the user wants to provision a Translation Pattern on Unified CM. If the template contains both a Route and Translation Pattern element, only the Translation Pattern is provisioned on Unified CM.</p>
Apply To	An indication of which devices the Number Translation should be applied to.	<p>Selection options in the drop-down list:</p> <ul style="list-style-type: none"> • IPPBX (i.e. Unified CM) • Transit (i.e. PGW) • IPPBX and Transit (i.e. both Unified CM and PGW)

Field	Notes	Remarks
Calling Line ID Presentation Name	An indication of whether the calling line's ID presentation name should be visible after number translation is applied.	Selection options in the drop-down list: <ul style="list-style-type: none"> • Default - if you do not want to change the calling line ID presentation name. • Allowed - if you want to display the calling line ID presentation name. • Restricted - if you want to block the display of the calling line ID presentation name.
Calling Line ID Presentation Number	An indication of whether the calling line's ID presentation number should be visible after number translation is applied.	Selection options in the drop-down list: <ul style="list-style-type: none"> • Default - if you do not want to change the calling line ID presentation number. • Allowed - if you want to display the calling line ID presentation number. • Restricted - if you want to block the display of the calling line ID presentation number.

Step 4 Click the **Add** button.

On clicking the **Add** button, the following back-end transactions are triggered:

- *AddCustomerNumberTranslation* or *AddLocationNumberTranslation*.
- *Driver_AddOrganisationNumberTranslation* or *Driver_AddLocationNumberTranslation* - these transactions provision the relevant Unified CM and PGW devices.

Notes on Device Provisioning

- *Customer*: Customer scoped number translations are provisioned to each Unified CM and/or PGW used by the customer i.e. for all Unified CMs/PGWs associated with the locations belonging to the customer. Each device is only provisioned once even if the same device is associated with two different locations.
- *All Locations*: These number translations are provisioned for each location belonging to the customer. If new locations are added all existing 'All Locations' number translations are provisioned for the new location. When a location is deleted all existing 'All Locations' number translations are again removed from the associated Unified CM.
- *Locations*: For a location scoped number translation only the associated Unified CM is provisioned.

Validation when Adding Number Translations

- Front-end validation is done on the existence and format of the values entered or selected for each field. Error messages appear in red below each field.
- Back-end validation includes:

- Existence checks are done before adding/modifying/deleting a Number Translation i.e. do not add if already existing, do not modify/delete if not existing.
- Validation is done to make sure that the same Number Translation with target 'Location' and target 'All Locations' cannot exist together.

Note

No validation is done to check how the number translation affects the dial plan. Only the pre-/post translation numbers are checked for validity.

Procedure

Modifying Number Translations

To modify the Number Translations for a specific Customer or Location:

- Step 1** Browse to *General Administration > Number Translation*.
- Step 2** For a Customer administrator all the number translations for the relevant Customer and all its Locations are displayed. For a Location administrator only the number translations for that location display. Click on the relevant *Pre-translated Number* (active text link) to modify the Number Translation details.

The number of records displayed is dependent on the number selected in the *Max results* drop-down list - 10, 50 (default), 100, 500 or Unlimited. Click the **Next** button (if relevant) to view the next set of records. When there are no more records to display, the **Next** button does not function.

Click on the relevant *Pre-translated Number* (active text link) from the list to modify the selected number translation.

- Step 3** Modify the required fields.

Note

The *Target* and *Feature Configuration Template* fields cannot be modified.

- Step 4** Click the **Modify** button.

On clicking the **Modify** button, the following back-end transactions are triggered:

- ModCustomerNumberTranslation or ModLocationNumberTranslation.
 - Driver_ModCustomerNumberTranslation or Driver_ModLocationNumberTranslation - these transactions modify the Number Translation on the relevant Unified CM and PGW devices.
-

Procedure

Deleting Number Translations

To delete Number Translations for a specific Customer or Location:

- Step 1** Browse to *General Administration > Number Translation*.
- Step 2** Select the relevant *Pre-translated Number* (active text link) that you want to delete.
- Step 3** Click the **Delete** button.

On clicking the **Delete** button, the following back-end transactions are triggered:

- DelCustomerNumberTranslation or DelLocationNumberTranslation.

- Driver_DelCustomerNumberTranslation or Driver_DelLocationNumberTranslation - these transactions remove the Number Translation from the relevant Cisco Unified Communications Manager and PGW devices.

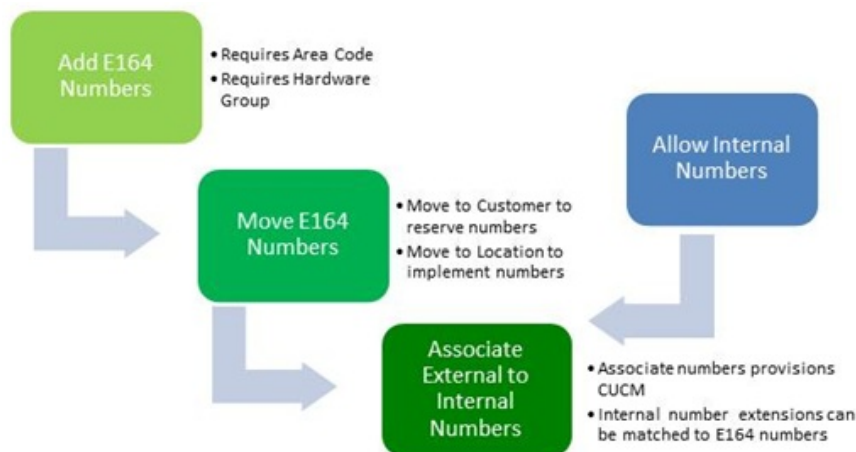
Bulk Loading Number Translations

- Bulk loading of Number Translations is done via the *Add Customer Number Translation* bulk loader (incorporated into the sample Resources workbook) or the *Add Location Number Translation* bulk loader (incorporated into the sample LocAdmin workbook).
- Multiple customer/location number translation mappings can be added at a time.
- For more information on bulk loading, refer to the *Bulk Loader Guide*.

E164 Numbers

The management of E164 is part of the process to add and move a range of E164 numbers to a location and then to associate the numbers to a range of internal numbers, which can be allocated to devices and users.

The figure below illustrates the process of adding and moving numbers.



E164 numbers, also called PSTN, DDI or DID numbers, are used to identify a phone to the outside PSTN world so that anyone can call the phone by dialing the E164 number. E164 Number Ranges can be added and moved using either the GUI or a bulk loader.

To work with the E164 Inventory, a country name for the section *Country Selection* and area code for *Defined Area Codes for Country* are required and need to be specified. For details, see:

- [Area Code Management on page 572](#)
- [Specifying the Area Code on page 574](#)

Important points about E164 numbers

- **E164 numbers are a limited resource and must be unique.** They cannot be created and used on an IPT platform without permission from the local PTT or regulatory authority. E164 numbers are allocated to telephony carriers by the regulatory authority and only the allocated number range can be created on the system.
- **Area Codes.** Area Codes are required to ensure that the E164 numbers you are working with are compliant with the specific region being managed. The Area Code prefix is required to be added to the E164 number in order to reach the Phone. See step 2 in [Pre-requisites for adding E164 numbers on page 571](#) for links to more detailed information that explains the concept of area codes, as well as area code management.

- **E164 numbers must conform to the country's standard digit length and starting digits.** For example geographic number consistency is normally a requirement, but the system can manage non-geographic numbers.
- **E164 number ranges.** E164 numbers can be managed in ranges, or as individual numbers. In many cases number ranges within a location will not be sequential, resulting in multiple number ranges having to be managed.
- **Numbers cannot be duplicated.** An inventory management system is essential in order to ensure that the same number is not assigned twice. Numbers are tracked by this system at each management level performs this inventory management task, and ensures that an E164 number cannot be allocated twice.

Note

Only a Provider administrator can move a number range from one customer location to another, or back to the inventory.

- **Managing E164 numbers.** E164 numbers can only be added by an administrator at the Provider level. And E164 numbers can **only** be moved to a location by an administrator at the Provider level. For example, a Provider administrator can move E164 numbers from the provider to a customer location, but a customer administrator cannot move E164 numbers from the provider level to the customer location level.
- An E164 inventory can belong to any of the following hierarchy levels and their administrator users: Provider, Reseller, Customer.

Ownership of numbers can be assigned in two different ways - when creating the number and when moving the number. For example, a number created by a provider administrator and then moved to a customer assigns ownership of the number to the customer administrator. When a customer moves the number to a reseller, the ownership of the number changes to the reseller.

When a number belongs to a customer it also belongs to the provider and reseller of that customer. All three parties are then allowed to move or delete the number.

- **Location Management.** E164 numbers only become active within the Unified CM once they have been moved to a Location and associated to an internal number. Before this, the E164 numbers are inventory items and are not present in the Unified CM.

Pre-requisites for adding E164 numbers

Before adding E164 numbers, the following processes (see table below) must be performed in the sequence provided:

Step	Brief Description / Remarks	Detailed Information (Where?)
1.	Country Codes. Make sure that country codes have been added at the base resource level. Note: This can only be done at either the Global (Dial Plan menu) or Provider (Provider Administration menu) level.	Country Management on page 46
2.	National Area Code. Make sure that the appropriate area code has been added to the relevant country.	Adding an Area Code on page 573 Area Code Management on page 768
3.	Hardware Group. Make sure that the relevant hardware groups have been added. Note: This must be done at the Provider Administration level or higher.	Add a Hardware Group on page 144

Step	Brief Description / Remarks	Detailed Information (Where?)
4.	Inventory Levels. Make sure that the number inventory levels have been correctly set at the Customer and Location levels before trying to move the numbers into the required location.	Specifying the Area Code on page 574

Using the GUI

The use of the GUI to carry out two management processes are described below:

- [Area Code Management on page 572](#)
- [Managing E164 Numbers on page 574](#)

The table below provides a summary and references to number range management:

No.	Process	Cross-reference	Remarks
1.	Add an E164 Number Range	Add E164 Number Range on page 576.	E164 numbers can only be used in the system once they have been moved to the required customer location as described below.
2.	Move an E164 number range	Move Number Range on page 578.	This process creates external numbers within the location.
3.	Internal Number (Extension) Range Management	Managing Available Internal Numbers on page 431	Note <ul style="list-style-type: none"> • Without available extensions, phone numbers are not available in the location. • The system allows an administrator to add only the number range that will be used. This would typically be to match the last digits within the E164 number range to be allocated to that location, for example 776 4010 associated with 4010).
4.	External Number Range Management	External Numbers Range Management on page 827	This process associates external numbers to internal numbers (extensions), and is a key step to ensure that extensions can be dialed directly from an outside (external) location.

Area Code Management

Area Codes define the geographic area for E164 numbers. The Area Code prefix is required to be added to the E164 number in order to reach the Phone. The *Area Code Management* page lists all of the National Codes for the country you selected from the drop-down list on the E164 Telephone Numbers page. To change the selected Country, browse back to the E164 Telephone Numbers page and select the required country. The list of National Area codes consists of two columns, one listing the National Area Codes and the other denotes whether the Area Code is Geographic or Non-Geographic.

[Adding an Area Code on page 573](#)
Procedure

Deleting an Area Code

To delete an area code:

- Step 1** Browse to *Resources > E164 Inventory*.
 - Step 2** Select the **country** from which you would like to delete an area code from then select the **Next** button.
 - Step 3** Select the **Area Code Mgt** button.
 - Step 4** Select the **Delete** button adjacent to the relevant Area Code.
-

The area code will be deleted from the system.

Note

- Only area codes that are not in use by the E164 inventory can be deleted. Before deleting an area code, please ensure that all references to the area code are removed (i.e. locations etc.).
 - An administrator cannot delete area codes created by administrators of a higher hierarchy level.
 - The Manage Area Codes screen displays the hierarchy entity (Provider, Reseller, Customer) of the administrator who added the area code, as well as the other associated hierarchy entities.
-

Adding an Area Code

Before you can create an inventory of E164 numbers, you must configure area codes and have a range of numbers allocated to the area codes.

Procedure

To add an area code:

- Step 1** Browse to *Resources > E164 Inventory*.
 - Step 2** Select a country to which you would like to add an area code then click the **Next** button.
 - Step 3** Click the **Area Code Mgt** button.
 - Step 4** Click the **Add** button.
 - Step 5** Enter the required area code and click the **Add** button. The area code is added to the system.
-

Note

- This procedure needs to be repeated for all required area codes.
 - The same area code can exist across different customers and only once per reseller.
 - The administrator user can not add codes that exist at a level higher than the level he belongs to, for example a customer administrator cannot add a code that already exists for his Reseller or Provider.
-

Specifying the Area Code

Before managing your E164 numbers, the system requires you to confirm the Area Code that you will be managing. This is to ensure that the E164 numbers you are working with are compliant with the specific region being managed.

Procedure

Follow these steps to specify the required national area code:

- Select the relevant national area code from the drop-down list and then select the **Next** button.

If you need to manage your national area codes, select the **Area Code Mgt.** button. For more information on Area Management, please see the [Area Code Management on page 572](#) Information page.

Managing E164 Numbers

E164 numbers are always linked to a country and an area (national) code. Therefore, in order to manage E164, you first need to define these details.

E164 numbers can be searched for from any point in the hierarchy. However, the system will present only the E164s available for the level of the hierarchy present and below. Therefore, when searching for E164 numbers, verify that the provider level of the hierarchy is being used.

Finding E164 Numbers

Procedure

- Step 1** Select *E164 Inventory* on the *Resources* menu. The country selection screen will appear.

Note

The system needs to understand which country rules to apply to the E164 number range.

- Step 2** Select the *country* you are working in from the drop-down list, and click the **Next** button. The area code selection screen will appear.

Note

If there is only one country defined in the system it will be the default country in the drop-down list. However, as the system is capable of supporting multiple countries in parallel, there may be more than one country in this list depending on the specific system configuration being used.

- Step 3** Select the applicable *Area Code* from the drop-down list and click the **Next** button. The list of DDI numbers configured for the area code will appear.

Note

- In some countries, area codes are not in use, so the system also supports a 'none' value.
- The **Area Code Mgt** button, at the top-left hand side of the page, goes to the Area Code Management page, which allows the addition of a new area code or to manage the area codes. (See [Adding an Area Code on page 573](#) for more details.)

- Step 4** To find a specific E164 or reduce the list, use the following search:

- **Number ends with:** all or part of the last digits in the E164 number

- **Number starts with:** all or part of the first digits in the E164 number
- **User Data:** Search using the optional user data field.
- **Unallocated:** E164 numbers which are not allocated to any location and are available at the provider level only
- **Allocated to location:** E164 number which have been allocated (moved) to a location

The following fields are presented for each E164 number:

Field	Notes	Remarks
Country	ISO country code and country name.	-
National area code	Area code prefix for the PSTN number.	-
Non geographic	Indicates if the area code is defined as non-geographic.	Y = Non geographic N = Geographic
E.164 number	The PSTN number.	-
Extension number	If the PSTN is mapped to an internal extension.	Only E164's which are allocated to location can be mapped to extensions.
Hardware Group Name	The hardware group used for the E164 number.	For example, HG-Locations-CUST-1-CUCM1.
Provider	The provider associated with the number.	-
Reseller	The reseller associated with the number.	-
Customer	The customer associated with the number.	-
Division	The division associated with the number.	-
Location	The location associated with the number.	-
Device Group	The device group related to the number.	-
User Data	Each E164 inventory entry can be assigned a user data field. This enables operators to track E164 numbers against contractual requirements.	This is an optional field.

Add E164 Numbers

The system allows for the option to add a single E164 number or a range of numbers.

Procedure

- Step 1** Follow steps under [Managing E164 Numbers on page 574](#) if required to get to the screen above. On the E164 list page, click the **Add Number** button.
- Step 2** Update the values for the new E164 number as required and click the **Add** button. The following fields are available:

Field	Notes	Remarks
Country	ISO country code and country name.	-
National Area Code	Area code prefix for the PSTN number.	<p>By default the area code presented is the one to select while going through the steps getting to the E164 List. However, if the number to be added is of a different area code, the system allows it to be changed by selecting from the drop-down list. This is a mandatory field.</p> <p>Notes:</p> <p>The system automatically adds the area code to the area codes list if it does not yet exist in the system.</p> <p>Even if the country dial plan requires a leading digit for calling with an area code, in this screen, it should be written without any leading digits.</p>
Local Number (in this Area)	The E164 number in the area code. This is a mandatory field.	-
Select a Hardware Group	The hardware group to which this number will be added.	<p>Select from a drop-down list. This is a mandatory field. The available options match the hierarchy of the user adding the E164 number. The hardware group selected must have one (or both) of the Location Gateways checkboxes (<i>Location Local Gateways</i> and/or <i>Location SRST Gateways</i>) selected.</p> <p>The hardware group is used to allow the concept of control over which hardware is updated when transactions against this E164 number is run.</p>
User Data	Each E164 inventory entry can be assigned a user data field. This enables operators to track E164 numbers against contractual requirements.	This is an optional field.

Add E164 Number Range

To add an E164 Number Range:

Procedure

- Step 1** Follow steps under [Managing E164 Numbers on page 574](#) if required to get to the screen above. On the E164 list page, click the **Add Number Range** button.

Step 2 Update the values for the new E164 number range as required and click the **Add** button. The following fields are available:

Field	Description	Remarks
Country	ISO country code and country name.	Read-only field.
National area code	Area code prefix for the PSTN number.	<p>This is a mandatory field. By default the area code presented is the one to select while going through the steps getting to the E164 List. However, if the number to be added is of a different area code, the system allows it to be changed.</p> <p>Notes:</p> <p>The system automatically adds the area code to the area codes list if it does not yet exist in the system.</p> <p>Even if the country dial plan requires a leading digit for calling with an area code, in this screen, it should be written without any leading digits.</p>
Start of number range	The first number in the required range.	This is a mandatory field.-
End of number range	The last number in the required range.	This is a mandatory field.
Select a Hardware Group	The hardware group to which these numbers will be added.	<p>Select from the drop-down list. This is a mandatory field. The hardware group selected must have one (or both) of the Location Gateways checkboxes (<i>Location Local Gateways</i> and/or <i>Location SRST Gateways</i>) selected (see View and Delete a Hardware Group on page 147 if required).</p> <p>The hardware group is used to allow the concept of control over which hardware is updated when transactions against the E164 numbers are run.</p>
User Data	Each E164 inventory entry can be assigned a user data field. This enables operators to track E164 numbers against contractual requirements.	<p>This is an optional field.</p> <p>The value supplied in the User Data field is applied to all of the numbers within the range.</p>

See also: [Managing E164 Numbers](#) on page 574.

Delete E164 Number Range

To delete an E164 Number Range:

Procedure

- Step 1** Follow steps in [Managing E164 Numbers on page 574](#) to get to the screen above. On the E164 list page, click the **Delete Number Range** button.
- Step 2** Select the first number in the range you wish to delete and the last number in the range from the drop-down lists on the screen. Then click the **Delete** button.
-

Note

The system allows you to delete a range even if some of the numbers in it cannot be deleted as they are allocated to a location. The system deletes only the numbers which are available for deletion, leaving the allocated numbers in the range in the system.

Move Number Range

Before an E164 number can be used in the system it needs to be allocated to a customer's location. This requires you to move the number to the required location. The system also allows provider, customer and reseller administrators to move numbers to other associated hierarchy entities below their own hierarchy level.

This screen can also be used to move numbers back to the phone inventory of the selected hierarchy of the logged in user.

Procedure

- Step 1** Follow steps in [Managing E164 Numbers on page 574](#) to get to the screen above. On the *E164 Telephone Numbers* screen page, click the **Move Number Range** button.

Note

When attempting to move numbers back to the selected hierarchy of the logged in user, if there are numbers in the range that are already associated and the "Skip associated numbers" checkbox is not selected, the transaction will fail.

- Step 2** Enter the relevant fields (see table below) and click the **Move** button. All numbers in the range that are not already associated are moved to the target location.

Field	Notes	Remarks
Select Target	The hierarchy entity to move numbers to.	<p>Select from the drop-down list of hierarchy entities associated with the provider. The options exclude divisions because division administrators are not allowed to manage the E164 inventory. Note that if the <i>Unassigned</i> option is selected, the selected number range is moved to the phone inventory at the highest point in the hierarchy of the logged in user.</p> <p>Note</p> <p>The system allows the moving of numbers to a Voicemail service, even when the Voicemail service is in a different country to the FNNs being moved.</p>
Start of number range	First number in the range to be moved	<p>Select from the drop-down list.</p> <p>The numbers available in the drop-down list are the numbers available in the phone inventory at the respective point in the hierarchy, for example at the selected customer or customer location. Note that the word "associated" is adjacent to numbers that are already associated in the phone inventory at the respective point in the hierarchy.</p>
End of number range	Last number in the range to be moved	<p>Select from the drop-down list.</p> <p>The numbers available in the drop-down list are the numbers available in the phone inventory at the respective point in the hierarchy, for example at the selected customer or customer location. Note that the word "associated" is adjacent to numbers that are already associated in the phone inventory at the respective point in the hierarchy.</p>
Skip associated numbers	This checkbox is only relevant when moving a number range back to the phone inventory of the selected hierarchy of the logged in user.	Select the checkbox to skip numbers that are already associated with the location, that is only unassociated numbers in the range are moved to the target location.

Using Bulk Loaders

To expedite the process of managing E164 numbers (as described under *Using the GUI* above), a bulk loader can be used at the provider level. See the Bulk Loader Guide for more information.

In this manner, the bulk loader performs multiple process steps as a single process instead of series of individual steps. The following bulk loader sheets can be used.

Note

- E164 numbers can only be added and moved by an administrator at the Provider level.
- E164 numbers can only be used in the system once they have been moved to the required customer location.

-
- **Add PSTN Number Ranges (Resources spreadsheet):** This sheet is used to add PSTN number ranges to the system.
 - **Move PSTN Number Range (LocAdmin spreadsheet):** This sheet is used to move a PSTN Number Range to a Location.
 - **Create Internal Number Range (LocAdmin spreadsheet):** This sheet is used to create an internal number range in a Location.
 - **Associate PSTN Number Range (LocAdmin spreadsheet):** This sheet is used to associate PSTN number ranges.

Note

In the sample sheet, the AssociateFNNinRanges preference setting for Auto_Loc is enabled; therefore, the extension ranges to be associated can only be added in powers of 10.

If required, end users (or lines) associated to end users can be added to telephony groups using the following bulk loader sheets:

- **Add Number Group (LocAdmin spreadsheet):** This sheet is used to add a number group to the system. Each row represents a new number group and the columns are used to specify characteristics such as the provider, number group name and the relevant lines.
- **Add Hunt Group (LocAdmin spreadsheet):** This sheet is used to add a hunt group to the system. Each row represents a new hunt group and the columns are used to specify characteristics such as the provider, hunt group name and the relevant lines.
- **Add Pickup Group (LocAdmin spreadsheet):** This sheet is used to add a pickup group to the system. Each row represents a new pickup group and the columns are used to specify characteristics such as the provider, pickup group name and the relevant lines.

See also:

- *Associate PSTN Number Ranges and Connect Location* in the Bulk Loader Guide for more information on associating PSTN number ranges.

Related topics to E164 numbers

- Internal Number Format

This is used to determine the format of the internal numbers (fints) in the system and the length. See [Internal Number Format on page 552](#) for more details if required.

- Disassociating Range of External Numbers

For details on how to disassociate a range of external numbers, see [Disassociating Range of External Numbers on page 829](#).

- Associate FNN Transaction

The AssociateFNN transaction handles the mapping of external numbers (also known as FNNs) to internal numbers (also known as FINTs). See [AssociateFNN on page 363](#) for more details. See also the Associate FNN Guide for a more in-depth description of this transaction.

- AssociateFnnInRanges

A location settings tool - *AssociateFnnInRanges*, is available from the *General Administration / Locations / Preference and Settings* screen.

If the preference is set on, the Association and Disassociation of FNNs in the PGW is done in set ranges. The ranges available are of 1, 10, 100, 1000 numbers. This allows for a much faster association/disassociation process, however, once the preference is set on and any association is done, the system prevents you from turning it off until all ranges of FNNs in this location are disassociated.

- Bulk Loader Guide
- Web Services API Guide

Forced Authorization Codes

Forced Authorization Codes (FACs) allow you to manage call access and accounting. This feature regulates the types of calls that certain users can place by forcing the user to enter a valid authorization code before the call completes.

FACs are configured as resources by selecting *Resources > Authorization Codes*. Each FAC has three items of data associated with it:

- A unique name
- Authorization Level (0 to 255)
- The code itself (up to 16 digits)

In the Unified CM model, the route pattern worksheet supports two columns for each route pattern:

Cisco Unified Communications Manager (Unified CM) Model

- **Require Forced Authorization Code:** Defaults to False
- **Authorization Level:** Defaults to 0

These will apply the relevant setting to the route pattern when it is loaded into the Unified CM.

Device Groups

Once a FAC has been assigned to a Location, it can be allocated to a Device Group.

Important

Device Groups must be enabled for this functionality to work.

Procedure

To allocate an FAC to a Device Group:

- Step 1** Browse to General Administration > Locations.
- Step 2** Select the relevant Location.

Step 3 Select the **Device Groups** button.

Important

If the installation has redefined the name to be used for Device Groups, an alternative name, for example *Tenants*, appears on the button instead of *Device Groups*.

Step 4 Select the required Device Group and then select the **Number of Forced Authorization Codes** link.

Step 5 A screen listing the available FACs and those already assigned to the Device Group appears. FACs can be assigned or removed from the Device Group using the FAC name and the **Assign >>** or **<< Remove** button as appropriate.

Note

Assigning a FAC to a Device Group does not affect the configuration in the Unified CM.

Additional Information

See also: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_1_1/ccmcfg/b03fac.html

Add FAC

A sequential range of FACs may be added to the system in a single operation. All the codes in a range have the same Authorization Level. They also have the same name, with the FAC appended to the name to differentiate them.

Procedure

To add a range of FACS:

Step 1 Browse to *Resources > Authorization Codes*.

Step 2 Click the **Add range** button.

Step 3 Complete the required fields.

Important: All fields are mandatory

The following fields are available:

Field	Description
<i>Range Start</i>	The first code within the range, this field can be up to 16 digits.
<i>Name</i>	The name of the range.
<i>Level</i>	The user level that the range will control.
<i>Range Size</i>	The number of codes available within the range.

Step 4 Click the **Add range** button.

The range is added to the system.

Note

- All of the codes in the new range have the same Authorization Level.

- All of the codes also have the same name, with the FAC appended to each name to differentiate them.

Assign FAC

FACs that have been created as resources may be assigned to Locations.

Procedure

To assign FACs to locations:

- Step 1** Browse to *Resources > Authorization Codes*.
- Step 2** Select the **Assign** link adjacent to the FAC to be assigned.
- Step 3** Specify the **Range Size** required and select the required **Location** from the drop-down list.
- Step 4** Click the **Assign Range** button.

The specified range of authorization codes is assigned to the specified Location.

Note

A number of adjacent sequential FACs may be assigned to the same Location in a single operation.

Release FAC

To release a FAC from a Location, select the *Release* link. This removes the FAC from the Unified CM.

Delete FAC

A FAC may be deleted by selecting the *Delete* checkbox and then clicking the **Apply** button. Several FACs may be deleted in a single operation by selecting the relevant *Delete* checkboxes before clicking the **Apply** button. If a FAC that is assigned to a Location is deleted, then it is automatically released from the Location and removed from the Unified CM before the resource is deleted.

Customer Specific Button and Softkey Templates

This section covers Button Group Management and Manual Mode Additions.

Button Group Management

Phone Button Template Groups and Softkey Template Groups are system wide resources. They are used to create sets of templates that may be used by individual Customers.

Individual Phone Button Templates are added to the system and managed by browsing to *Setup Tools > Phone Types* and selecting *Phone Type Management*. Softkey Templates are imported from the Cisco Unified Communications Manager (Unified CMs) attached to the system. To view softkey templates, browse to *Network > PBX Devices*, select the relevant CCM Cluster Name (active text link), then click the *Import/Refresh Items* button, and then select the *Softkey Templates* active text link.

Note

- Line assignments, busy lamp fields (BLFs), speed dials and service URLs are supported by Phone Button Templates.
 - Enterprise-level IP Phone Service subscriptions cannot be assigned to a phone button template service URL. This is a limitation of the Unified CM and not Cisco Unified Communications Domain Manager (CUCDM).
 - A single user-level IP Phone Service subscription can be mapped to multiple phone button template service URLs.
 - In order to delete a user-level IP Phone Service, all phone button template service URLs assigned to this service must be deleted. Two Operations Tools have been added to help facilitate this process:
 - Delete All Service URL buttons for Users at Location - This operation removes all phone button template service URLs for extension mobility profiles at a specific location.
 - Delete All Service URL buttons for Devices at Location - This operation removes all phone button template service URLs for devices at a specific location.
-

Add a Phone Button Template Group

Individual Phone Button Templates enable administrators to create and modify highly detailed templates that dictate the functions of a phone's buttons.

Procedure

Add Phone Button Template Group

To add a Phone Button Template Group:

- Step 1** Browse to *Setup Tools > Button Groups > Phone Button Template Groups*.
- Step 2** Click the **Add** button.
- Step 3** Enter the unique name for the group and an optional description, then click the **Add** button.
-

The Phone Button Template Group is added to the system.

View and Modify Button Group Templates

Individual Phone Button Templates enable administrators to create and modify highly detailed templates that dictate the functions of a phone's buttons.

Procedure

Assign Phone Button Templates to a Group

To assign Phone Button Templates to a Group:

- Step 1** Browse to *Setup Tools > Button Groups > Phone Button Template Groups*.
- Step 2** Select the *Group Name* (active text link) of the template group that you would like to assign templates to.

- Step 3** The screen shows two boxes, the left hand side is a list of available Phone Button Templates and the right has a list of templates that have already been assigned to the group
- Templates may be assigned to, or removed from, the group by selecting the template name(s) and clicking the **Assign** >> or << **Remove** button as appropriate.

- Step 4** Once you have finished selecting templates, click the **Modify** button.

The Button Template Group is modified in the system.

Note

A template may be a member of multiple groups.

Procedure

Delete Phone Button Template Group

To delete a Phone Button Template Group:

- Step 1** Browse to *Setup Tools > Button Groups > Phone Button Template Groups*.
- Step 2** Select the *Group Name* (active text link) of the template group that you would like to delete.
- Step 3** Click the **Delete** button.

After confirming the deletion, the Button Template Group is removed from the system.

Procedure

Assigning Template Groups to a Customer

To assign Phone Button Template Groups to a customer:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the *Name* (active text link) of the Customer that you would like to assign templates to.
- Step 3** In the button Groups section there are two drop-down selection boxes, one for the *Phone Button Template Groups*, the other for *Softkey Template Groups*. If a group is selected, only templates from that group are available for use by that Customer. If the *default* option is selected, any template may be used.
- Step 4** After making your group selections, click the **Modify** button.

The customers template groups are modified in the system.

Using Phone Button Template Groups

Phone Button Templates are used when moving, registering, managing phones and for mobility profiles. Only those templates that are members of the group selected for the specific Customer may be used. If the Customer selection was the *default* group, any phone button template may be used. To assign button template groups to a customer, follow the steps below.

Add a Soft Key Template Group

Softkey Templates are imported from the Cisco Unified Communication Manager (Unified CM) attached to the system. These templates enable administrators to customize the functions of a phones softkeys.

Procedure

Add Softkey Template Group

To add a Softkey Template Group:

- Step 1** Browse to *Setup Tools > Button Groups > Softkey Template Groups*.
 - Step 2** Click the **Add** button.
 - Step 3** Enter a unique name for the group and an optional description, then click the **Add** button.
-

The new Soft key Template group is added to the system

View and Modify Softkey Templates

Softkey templates are imported from the Unified CMs attached to the system. These templates enable administrators to customize the functions of a phones softkeys.

Procedure

Assigning Soft key Templates to a Group

To assign soft key templates to a group:

- Step 1** Browse to *Setup Tools > Button Groups > Softkey Template Groups*.
 - Step 2** Select the *Group Name* (active text link) of the Template Group that you would like to assign templates to.
 - Step 3** The screen shows two boxes, the left is the list of available Softkey Templates and on the right is the list of those that have already been assigned to this group. Templates may be assigned to, or removed, from the group by selecting the template name(s) and click the **Assign >>** or **<< Remove** button as appropriate.
 - Step 4** Once you have finished assigning templates, click the **Modify** button to confirm the changes.
-

The Soft key Templates group is modified in the system.

Note

A template may be present in multiple groups.

Procedure

Delete Softkey Template Group

To remove a Softkey Template Group:

- Step 1** Browse to *Setup Tools > Button Groups > Softkey Template Groups*.
 - Step 2** Select the *Group Name* (active text link) of the Softkey Template that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the delete operation, the Softkey Template group is removed from the system.

Assigning Softkey Groups to a Customer

The same process used to assign phone button template groups to customers is used to assign Softkey template groups to customers. For information, please see the Assigning Phone button Groups to a Customer section.

Using Softkey Template Groups

Softkey Templates are used when moving, registering, managing phones and working with mobility profiles. Only the templates that are members of the group selected for the Customer, and are available in the Location's Unified CM, may be used. If the Customer selection was the *default* softkey group, then any softkey template available on the Location's Unified CM may be used. If the Location's Unified CM is in unmanaged (manual) mode, then any softkey template may be selected.

Emergency DDI

In the current Hosted UCS solution, when an Emergency call is made from an IP Phone configured in the Hosted UCS IP Location, the CLI passed to the emergency operator is always the DDI configured in the Emergency Number Management page of the Location. (*General Administration -> Locations -> <LocationX> -> Advanced Mgt.-> Emergency Number*) and is known as the Location Emergency Published Number (LEPN). This was enhanced so that if an emergency calls is initiated from endpoints configured with a DDI, the DDI can optionally be passed to the emergency operator as the CLI.

The decision whether to use configured IP Phone DDI or the LEPN is also dependent on whether a call is routed to Central or Local PSTN Breakout, and whether the DDI is a Geographic or Non-Geographic number.

There are four areas/levels in the GUI where EDDI can be changed to have an effect on the CLI passed to an emergency operator, namely Country, Customer, Location and FNN Range. At the Country level you can change the preference for Non Geographic numbers only, whether it's for Local or Central breakout. Country setting for local and central options can be *Device CLI* or *Published Number* .

Customer setting can be *Device CLI* or *Published Number* and Location setting can be *Derived From Customer* , *Device CLI* or *Published Number* , FNN Range will be used when External (E.164) numbers are associated with internal extensions.

The *EmergencyCLI* transaction is model driven with scripts *AssociateFNN-Emergency* and *DisAssociateFNN-Emergency* in the PGW TimesTen worksheet.

Country Setting

To change the Country setting, navigate to *Dial Plan Tools > Countries > <select country>* change the required setting and click the **Modify** button.

The Default for Local setting is *Device CLI* and the default setting for Central is *Published Number*. When any of these settings are toggled all the *Non Geographic* number associations are affected in all the Locations of the Country. An Emergency-CLI script will be run against the PGW-TimesTen database. The exact model for the transaction will be decided by the direction in which the preference was toggled, i.e. from *Published Number* to *Device CLI* or *Device CL I* to *Published Number* .

Customer Setting

To change the Customer setting, navigate to *General Administrator -> Customers -> <navigate to the customer maintenance screen> ->* then click the **Advanced Mgt.** button -> click the **Advance Telephony Settings** button.

Select required setting from the drop-down list box and click the **Apply** button. Options are *Published Number* and *Device CLI*. When the Customer setting is toggled all locations for the customer with an Emergency CLI preference of *Derived From Customer* will be searched. For every external to internal number association (FNN association) an Emergency-CLI script will be run against the *PGW-TimesTen* database. The exact model for the transaction will be decided by the direction in which the preference was toggled, i.e. from *Published Number* to *Device CLI* or *Device CLI* to *Published Number*.

Location setting

To change the Location setting, navigate to *General Administrator > Locations > <navigate to location maintenance screen> -> select the **Advanced Mgt.** button -> select the **Advance Telephony Settings** button.*

Select required setting from the drop-down list box and click the **Submit** button. Options are *Derived from Customer*, *Published Number* and *Device CLI*. When the Location setting is toggled, for every external to internal number association (FNN association) an Emergency-CLI script will be run against the *PGW-TimesTen* database.

The exact model for the transaction will be decided by the direction in which the preference was toggled, i.e. from *Published Number* to *Device CLI* or *Device CLI* to *Published Number*. If the *Derived from Customer* setting is selected the Customer preference will be used to decide which model to use.

FNN Range Setting

The FNN Range setting will be triggered when internal extensions are associated with external numbers. Navigate to *Location Administration > External Numbers <navigate from provider to location level>* click the **Associate Range** or **Disassociate Range** button.

For every external to internal number association (FNN association) an Emergency-CLI script will be run against the *PGW-TimesTen* database. The exact model for the transaction will be decided by the Associate or Disassociate button used. If the location's preference is *Derived From Customer* the Customer preference will be used to decide which model to use.

Authentication Management

When logging into the admin GUI users are authenticated against the internal system database, however when logging into Self Care, users can be authenticated against the internal system database, or an external authentication server (e.g. LDAP or Active Directory).

Self Care users are identified as LDAP/Active Directory users based on their security profile as configured in the system's admin GUI. This means that users identified as LDAP/Active Directory users will log in to Self Care using their LDAP/Active Directory usernames and passwords. For these users, authentication will be performed externally by an LDAP/Active Directory server. LDAP/Active Directory authentication and built-in authentication (internal) are mutually exclusive; i.e. an end user will use one or the other. If a user is authenticated via LDAP/Active Directory and this fails, then the user does not have a valid LDAP/Active Directory login. Alternatively a normal user will fail as per the existing login and password framework.

Authentication for Administrators will remain unchanged (it is not LDAP/Active Directory - enabled). Administrators will have the functionality to configure the various settings and options required to support LDAP/Active Directory authentication in Self Care.

For an end user to be authenticated via external authentication (e.g. LDAP or Active Directory), the following must be in place:

1. A Security Profile for external authentication must exist on the system.

2. An external authentication server (e.g. LDAP/Active Directory server) must be provisioned on the system, with correct server details, e.g. hostname, bind DN and bind password.
3. The authentication server must be associated with a system hierarchy level (s), to allow end users associated with that hierarchy level to be migrated to external authentication via the authentication server.
4. When the user logs in, the system must be able to connect to the external authentication server (using the configured settings) in order to authenticate the user.

No syncing functionality currently exists; therefore, the user must be provisioned in the system exactly the same as in the external authentication (LDAP) server (e.g. use the same case as on the external server).

End user authentication is a three-step process, outlined by the following:

1. The system will bind to the LDAP/Active Directory server using the *bind DN* and *bind password*. The bind DN is an account usually with read-only access to the part of the LDAP/Active Directory tree that stores user account information. It needs read access to the user's DN and the attribute that stores the username. The bind password is encrypted before it is stored in the system's database, and decrypted before it is used to bind to the server in order to not compromise security.
2. The LDAP/Active Directory server will search for the LDAP/Active Directory record of the user to be authenticated using the *username* provided by the Self Care user.
3. The LDAP/Active Directory server will check that the LDAP/Active Directory client can bind to the LDAP/Active Directory server using the user's DN and the *password* provided by the user.

Once authenticated, LDAP/Active Directory users bypass the functionality related to users whose passwords are managed by Self Care. Self Care does not interfere with LDAP/Active Directory account management. LDAP/Active Directory users cannot change their passwords via Self Care. Self Care never asks them to change their passwords, nor does it expire or disable passwords after a series of unsuccessful logins. All of this will be configured and managed by the LDAP/Active Directory server.

When using external authentication (e.g. LDAP/Active Directory), the password for the user is not stored in the system and will therefore not be provisioned for connecting to other related services or applications, e.g. Unity, Cisco Unified Communications Manager, etc. It is advisable to use the same external authentication server (e.g. LDAP/Active Directory) for user authentication of other services or applications as the external authentication server being used for the system.

Enable External Authentication in Security Profile

Procedure

To add a Security Profile:

- Step 1** Navigate to *Setup Tools > Security Profiles*.
- Step 2** Click the **Add** button.
- Step 3** Provide the *Profile Name*, *Description* and select the *Enable External authentication* field. When external authentication is enabled, it means that users linked to the Security Profile will be authenticated via an external authentication server, e.g. LDAP/Active Directory. On selection of the checkbox, all fields related to *authentication rules* are disabled as the applicable rules are managed by the external authentication server.
- Step 4** Click the **Add** button.

Authentication Management steps

Adding and Modifying an Authentication Server

[Adding an Authentication Server on page 590](#)

Procedure

Modifying an Authentication Server

To modify an Authentication Server:

- Step 1** Browse to *Network > Authentication Servers*.
- Step 2** Select the relevant Server Name.
- Step 3** Provide the updated details for the LDAP/Active Directory Authentication server.
- Step 4** Click the **Modify** button. The LDAP/Active Directory Authentication server's details will be modified in the system.

Adding an Authentication Server

Procedure

To add an Authentication Server:

- Step 1** Browse to *Network > Authentication Servers*.
- Step 2** Click the **Add** button.
- Step 3** On the next screen, click the **Add** button adjacent to the LDAP authentication type.
- Step 4** Provide the LDAP Authentication server's details. The following settings are available:

Field	Description
Hostname / FQDN	The hostname / Fully Qualified Domain Name of the server. Note The server's IP address can also be entered.
Bind DN or user	The Bind account's DN (distinguished name) or user details of the server.
Bind Password	The bind account password.
Connection Security	Select from the drop-down list one of the following values: 'None', 'SSL' or 'TLS'. The port defaults to '636' when selecting 'SSL' and defaults to '389' when selecting 'None' or 'TLS'.
Base DN	The base DN under which all user accounts can be found.
Administration Level	Select from the drop-down list the administration level to which the LDAP server is being added.
Port	The port number to be used when accessing the server. Optional field, defaults to a value of '389'.

Field	Description
Login Attribute	<p>The login attribute to be used when end-users authenticate against this server.</p> <p>Note</p> <p>When authenticating an <i>Active Directory</i> user, there are only two possible login attributes that can be used: <i>userPrincipalName</i> and <i>sAMAccountName</i>.</p> <p>However, the following values are possible for this field:</p> <ol style="list-style-type: none"> 1. uid/sAMAccountName 2. sAMAccountName 3. mail 4. employeeNumber 5. telephoneNumber 6. userPrincipalName <p>Since Unified CM supports more than one type of LDAP authentication server, these values are used as follows:</p> <ul style="list-style-type: none"> • 1 for authenticating against a Unix LDAP server. • 2 or 6 for authenticating against a Microsoft AD LDAP server. • In certain cases it may be desirable to use a different username to log into Selfcare with and authenticate to the LDAP server. 3, 4 or 5 can be used if that is the unique attribute that the authentication server has associated with the username. For example, log in to Selfcare with an telephone number (5), email address (3) or employee number (4) as a username and then pass that to the Authentication server as the unique attribute associated with the user. <p>While the uid/sAMAccountName is typically used for a Unix based LDAP implementation, you are not restricted to use it. In other words, if the LDAP schema on the LDAP server has been set up to use the telephone number, employee number, email address, etc. then you can use one of those instead.</p>
Domain Name	<p>The relevant domain name, e.g. example.com, to be used when Active Directory is the authentication server. In the case of openLDAP, this field should be left empty.</p> <p>Note</p> <p>When a domain name is provided, the domain name will be appended to a user's username at the time of logging in to Self Care. Therefore, a user with the name of 'bob' will be validated as 'bob@example.com'. However, providing a domain name will only result in successful login validation when the <i>Login Attribute</i> is '<i>userPrincipalName</i>'. When the Login Attribute is '<i>sAMAccountName</i>' a user called 'bob' will remain 'bob' on the authentication server, which means that the appended domain name will result in an incorrect username of 'bob@example.com'. Therefore, don't provide a <i>Domain Name</i> when the <i>Login Attribute</i> is '<i>sAMAccountName</i>'.</p>

- Step 5** Click the **Add LDAP Auth Server** button.

Note

If the level of the admin user who is adding the LDAP/Active Directory server is the same as the admin level of the LDAP/Active Directory server being added, then association to that level of the hierarchy will be carried out automatically, immediately after the LDAP/Active Directory server has been added. For more information on association, see [Associating an Authentication Server on page 592](#).

Associating an Authentication Server

Association of an external authentication server should not be confused with the administration level of the server. Administration level is defined upon the configuration of the external authentication server, and determines which level of admin (Provider Admin, Customer Admin, Location Admin, etc.) will be able to configure and associate the server. Association relates to the specific hierarchy element(s) that will use the external server. To illustrate:

- A server may be configured to be administered on Customer Level, which is to say a Customer Administrator will be able to modify the external authentication server settings and associate the server to a location, etc.
- The same server may then be associated to a location for example, which means that all users in that Location, with their security profile set to LDAP, will authenticate against the specific external authentication server.

The same authentication server definition can be associated to multiple hierarchy elements within the system, but a single hierarchy element can only have ONE authentication server definition associated. A location for example can only have a single authentication server associated to it, but it is possible to also associate said authentication server to another location.

Procedure

To associate an Authentication Server to the relevant hierarchy element(s):

- Step 1** Browse to *Network > Authentication Servers*.
- Step 2** Click the **Associate** button.
- Step 3** Select the relevant hierarchy element(s) from the *Not associated* list.
- Step 4** Click the **Add To List** button. The selected hierarchy element(s) will now appear on the *To be associated* list.
- To remove a hierarchy element(s) from the selection to be associated, select the relevant hierarchy element(s) from the *To be associated* list and click the **Remove from list** button.
- Step 5** After the relevant hierarchy element(s) have been added to the list to be associated, click the **Next** button.
- Step 6** Select the *Migrate Users* checkbox for the relevant hierarchy element(s) being associated to the LDAP/Active Directory server. This step will migrate all end users associated with the relevant hierarchy element(s) with an external security profile, to the LDAP/Active Directory authentication server.
- Step 7** Select the *Search up* field to *search up* the system hierarchy for LDAP/Active Directory servers to associate to. This allows an LDAP user to be authenticated against more than one LDAP/Active

Directory server configuration. See [Authentication Logic on page 593](#) for an explanation. (This field is optional and only available when the hierarchy being associated is at either Division / Location level. When this field is enabled the system will check for the existence of at least one associated authentication server higher up in the admin hierarchy. This check is performed up to the Customer level and any authentication servers available above that (Reseller, Provider) are ignored.)

Note

When a user is migrated to LDAP/Active Directory, the user's system password is cleared.

- Step 8** Click the **Associate Auth Server** button.

Disassociating an Authentication Server

Procedure

To disassociate an Authentication Server from the relevant administration level(s):

- Step 1** Browse to Network > Authentication.
- Step 2** Click the **Disassociate** button.
- Step 3** Select from the *Hierarchy Levels to Disassociate From* list the relevant hierarchy element(s) to disassociate.
- Step 4** Select the *Migrate Users* checkbox adjacent to the hierarchy element(s) you want to disassociate.
- Step 5** Select the *Search Up Users* checkbox adjacent to the administration level you want to disassociate.

Note

- Users are migrated from the LDAP security profile to the Default security profile. Make sure that the default Security Profile is not LDAP/Active Directory.
- Migrating users from LDAP/Active Directory sets the user's system password to the default password, namely 'password'.
- When the *Search Up Users* option is selected the system will check that there are no LDAP/Active Directory servers (from the customer hierarchy level down) associated.

- Step 6** Click the **Disassociate Auth Server** button.

Authentication Logic

When a user logs into Self Care, and said user has the LDAP security profile set, the user will authenticate against the authentication server associated to the hierarchy element closest to the user. If for example there is an authentication server associated to the location the user is in, the user will be authenticated against this server. If the location does not have an associated authentication server, then the next level up the hierarchy (Division) will be checked. If the division has an associated authentication server associated to it, then the user will authenticate against that server, if not, then the Customer will be checked for an associated authentication server, and so on up the hierarchy.

If the *Search up* flag for the Authentication Server was not selected when the association was done, it is important to note that once an authentication server has been found and authentication

has failed, no further searching will be done up the hierarchy. If an LDAP user for example logs into Self Care, and authentication fails against the server associated to his/her location, then even if a server is associated to the upstream division and/or customer, no attempt will be made to authenticate the user against any one of these servers.

If however, the *Search Up* flag was selected when the Authentication Server was associated, then authentication against a server higher up in the hierarchy will be attempted after authentication against the associated server has failed. If an LDAP user for example logs into Self Care, and authentication fails against the server associated to his/her location, and the *Search Up* was selected when the server was authenticated, then the user will be authenticated against an upstream server associated to his/her division or customer.

The *Search Up* functionality is limited to the Authentication Servers associated to the Customer level and lower only, which is to say that no attempt will be made to authenticate a user against any upstream servers higher than Customer level if authentication has already failed for said user. Say a self care user's authentication has failed on location level, and search up was enabled, and said user authentication also failed at division level, and there is no associated server at customer level, then authentication will fail, even if authentication servers have been associated at Reseller or Provider level. By the same token, if a user's authentication has failed on location level and again at Customer level (assuming no division level association), then no further authentication will be attempted, and login will fail.

LDAP Integration with Cisco Unified Communications Manager (Unified CM) and Cisco Unity Connection

The LDAP functionality was introduced in system release 7.3 in order to ensure that the system operates correctly when the Unified CM is using an LDAP directory to store user details. This feature also ensures that the system operates correctly when Cisco Unity Connection is using an LDAP directory to access user details.

Note

If Unified CM and Cisco Unity Connection are LDAP integrated, they do not allow you to create users or change passwords as this is handled via LDAP. This impacts on the system as it cannot add users via the AXL API.

Limitations

LDAP integration has the following known limitations:

- If a user is not found on the Cisco Unity Connection/Unified CM when the system is doing an add, the system fails the *AddUser* transaction with a message that states the user was not found on the Unified CM/Cisco Unity Connection. This is because the user is expected to already be on the server since LDAP is enabled.
- For system release 7.3.1: When deleting an LDAP integrated user, the system removes all the configuration associated with the user at the Unified CM/Cisco Unity Connection, but does not actually delete the user.
- For system release 7.4.11.2 and onwards: When deleting an LDAP integrated user from the system, the system removes all the configuration associated with the user at the Unified CM, but does not actually delete the user. The user's voicemail account and all information is fully deleted from Cisco Unity Connection.
- The Unified CM version needs to be 8.0 or later for this setup to function.
- The user details page (admin GUI and self-care) drives the following fields for a user in the Unified CM when the cluster serving the user's location is LDAP aware in CUCDM:

- The permission groups in Unified CM for CTI management are added to the user if the CTI enabled setting is true in CUCDM.
- The following fields are managed by CUCDM for a user in Cisco Unity Connection when the cluster serving the end user's location is LDAP aware:
 - List in Directory = based on Ex-Directory setting for the user. If Ex-Directory is checked, the list in directory is false. If ex-directory is unchecked, the list in directory setting is true.
 - self-enrolment flag = self-enrolment setting on the mailbox in CUCDM
 - dtmf-id = voicemail number format for the extension associated with the voicemail (driven by the number construction settings for voicemail number)
 - Voicemail pin = voicemail pin in CUCDM

Configuring LDAP Integration

To enable LDAP integration, configuration needs to occur within the system and on the Unified CM/Cisco Unity Connection.

System Configuration

For an Existing Cisco Unified Communications Manager (Unified CM)

Procedure

To configure the system for LDAP integration with an existing Unified CM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the relevant server.
- Step 3** Select the *LDAP Aware* checkbox.
- Step 4** Click the **Modify** button. LDAP integration is now enabled for the selected Unified CM.

Note

To disable LDAP integration, follow the steps above but uncheck the *LDAP Aware* checkbox.

For a New Cisco Unified Communications Manager (Unified CM)

Procedure

To configure the system for LDAP integration with a new Unified CM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the Unified CM server type.
- Step 4** Complete all of the required fields ensuring that the *LDAP Aware* checkbox is selected.
- Step 5** Click the **Add** button. LDAP integration is enabled and the Unified CM is added to the system.

Note

To disable LDAP integration, follow the steps in the *For an Existing Cisco Unified Communications Manager* section but uncheck the *LDAP Aware* checkbox.

Onboarding end users when Unified CM is LDAP integrated

The assumption is made that the Unified CM has been configured for LDAP integration.

Procedure

The following procedure needs to be followed when onboarding end users:

- Step 1** Add the end user into the LDAP directory that is accessible by Unified CM.
- Step 2** Perform a Full Synchronization of Unified CM with LDAP or configure the LDAP directory synchronization schedule to occur periodically. Wait for the LDAP synchronization with Unified CM to complete. Users added in LDAP are added into Unified CM once the synchronization process is completed.

Note

Unless a "Refresh" message is sent from the Unified CM cluster, it is necessary to wait until the next periodic synchronization before the users will be in Unified CM and be able to be added to CUCDM.

- Step 3** Add end users into CUCDM via one of the CUCDM interfaces (web service, bulk loader, administration user interface). When the user is added to CUCDM, it updates the user details in Unified CM modifying the fields supported as noted above.
- Step 4** Once the end user is successfully added to CUCDM, end user services can be added to CUCDM in the normal way.

Note

The user needs to be in Unified CM before you can add the user to CUCDM. If the user does not exist in Unified CM then the add end user transaction in CUCDM will fail with a message indicating that the Unified CM cluster is LDAP enabled but the user does not exist on it.

For an Existing Cisco Unity Connection Server

Procedure

To configure the system for LDAP integration with an existing Cisco Unity Connection Server:

- Step 1** Browse to *Network > Voicemail Servers*.
- Step 2** Select the *Name* (active text link) of the relevant server.
- Step 3** Select the *LDAP Aware* checkbox.
- Step 4** Click the **Modify** button. LDAP integration is now enabled for the selected Cisco Unity Connection Server.
-

Note

To disable LDAP integration, follow the steps above but uncheck the *LDAP Aware* checkbox.

For a New Cisco Unity Connection Server

Procedure

To configure the system for LDAP integration with a new *Cisco Unity Connection Server*:

- Step 1** Browse to *Network > Voicemail Servers*.
- Step 2** Click the **Add** button.
- Step 3** Click the **Add** button adjacent to the Cisco Unity Connection server type.
- Step 4** Complete all of the required fields ensuring that the *LDAP Aware* checkbox is selected.
- Step 5** Click the **Add** button. LDAP integration is now enabled and the Cisco Unity Connection server is added to the system.

Note

To disable LDAP integration, follow the steps in the *For an Existing Cisco Unity Connection Server* section but uncheck the *LDAP Aware* checkbox.

Considerations for onboarding end users when Cisco Unity Connection is LDAP integrated

The assumption is made that the Cisco Unity Connection has been configured for LDAP integration.

Procedure

The following procedure needs to be followed when onboarding users with a voicemail account:

- Step 1** Add the end user to the LDAP directory.
- Step 2** Perform a Full Synchronization of Cisco Unity Connection with LDAP or configure the LDAP directory synchronization schedule to occur periodically. Wait for the LDAP synchronization with Cisco Unity Connection to complete. Users added in LDAP are added to Cisco Unity Connection as importable users once the synchronization process is completed.

Note

Unless a "Refresh" message is sent from the Cisco Unity Connection cluster, it is necessary to wait until the next periodic synchronization before the users will be in Cisco Unity Connection and can be imported.

- Step 3** CUCDM 8.1.0 release and later will import users automatically into Cisco Unity Connection. For pre-8.1.0 CUCDM releases the import needs to be done manually. Import the users into Cisco Unity Connection ensuring that:
 - A voicemail template is selected that represents the voice mail features to be allocated to the user since the voicemail account is created once-off using this template.
 - Any unique extension number is selected. When adding a voicemail account for the end user in CUCDM this extension number is updated by CUCDM to the extension number specified in CUCDM.
- Step 4** Add a voicemail account for the end users in CUCDM using one of the CUCDM interfaces (web service, bulk loader, administration user interface). When the voicemail account is added to CUCDM, it performs a modify into the Cisco Unity Connection modifying the fields supported as noted above, including correcting the dtmf-id allocated to the user.

Note

- If the user is not imported when adding a voicemail account for the end user in CUCDM, the transaction will fail.
 - When adding voicemail accounts for end users the usernames will be accepted in any of three formats, namely the exact original format in LDAP, all characters in lower case, or all characters in upper case.
-

Considerations for off-boarding end users when Cisco Unity Connection is LDAP integrated

From CUCDM release 8.1.1, consideration is no longer needed for the order in which users are deleted from the LDAP directory, the timing of LDAP synchronization with Cisco Unity Connection and when the user is deleted from CUCDM. An LDAP integrated user's voicemail account can be removed from CUCDM before or after the end user is removed from the LDAP directory. The procedure for removing the voicemail account of an LDAP integrated end user's voicemail account is the same as that of a non-LDAP integrated end user.

Considerations for off-boarding end users when Unified CM is LDAP integrated

From CUCDM release 8.1.1, consideration is no longer needed for the order in which end users are deleted from the LDAP directory, the timing of LDAP synchronization with Unified CM and when end users or their services are deleted from CUCDM. LDAP integrated end users and their UC services can be removed from CUCDM before or after the end user is removed from the LDAP directory. The procedures for removing LDAP integrated end users and their UC services are the same as that of non-LDAP integrated end users.

Note

When an LDAP integrated end user is associated with a dual mode phone and the end user is deleted from the LDAP directory the end user and the dual mode phone are deleted from Unified CM when the Unified CM garbage collector process runs. When the dual mode phone is un-registered or disassociated from the end user in CUCDM, the CUCDM inventory will be synchronized with that of Unified CM, resulting in the dual mode phone being removed from the CUCDM phone inventory.

Considerations for modifying user details when Unified CM and/or Cisco Unity Connection is LDAP integrated

If the user details are changed in LDAP, these will be reflected in the Unified CM (for example, First name, last name, etc). These need to then be updated in CUCDM to have the latest details for the user. If this data gets out of sync, there are no technical issues (transactions will still work), but there will be inaccurate data in the system. The update in LDAP and CUCDM can happen in any order

Considerations for future migration to LDAP integrations

When CUCDM is deployed with Unified CM and Cisco Unity Connection that is NOT LDAP integrated, the following needs to be considered to ensure future migration of Unified CM and/or Cisco Unity Connection to a LDAP integrated configuration:

Note

It is recommended to export a list of the usernames in the LDAP directory and run a check that the usernames are the same as the users added to CUCDM.

- It is essential that end user names are added into CUCDM (and propagated to Unified CM and Cisco Unity Connection) match the usernames that are planned for use in active directory.
- Users in CUCDM, Unified CM, Cisco Unity Connection and any external systems but not in the LDAP directory need to be added to LDAP directory before configuring the system for LDAP integration.

Procedure

Following these checks perform the following procedure:

- Step 1** Configure LDAP synchronization on the Unified CM cluster and/or the Cisco Unity Connection cluster as per the above documentation and synchronize.
- Step 2** Configure the Unified CM and/or Cisco Unity Connection clusters in CUCDM to be LDAP aware.

Note

If the LDAP-aware is enabled in CUCDM, but the user data has not been synchronized to the Unified CM/Cisco Unity Connection, then user-based transactions will fail in CUCDM as the user data is not available.

Actions to take when the recommended procedure has not been followed

In the instance where the recommended procedures in this and related documents have not been adhered to, errors may occur in CUCDM. For example, this may occur when attempts are made to remove end users or end user services from CUCDM. These errors occur because the services are removed by the Unified CM using cascaded deleting of the services; with the end user being removed as part of the LDAP/Unified CM synchronisation operation.

The following steps outline how to successfully remove the user and related services from CUCDM when this configuration has been removed from the underlying UC applications:

Procedure

If the end user has presence enabled:

- Step 1** Put the presence server and the IPPBX in manual mode.
- Step 2** Delete presence service for the end user from CUCDM.
- Step 3** Take the presence server and the IPPBX out of manual mode.
-

Procedure

If end user has mobile identity enabled:

- Step 1** Put the IPPBX in manual mode.
- Step 2** Delete mobile identities of the end user from CUCDM.
- Step 3** Take the IPPBX out of manual mode.
-

Procedure

If end user has single number reach enabled:

- Step 1** Put the IPPBX in manual mode.
 - Step 2** Delete remote destinations and single number reach for the end user from CUCDM.
 - Step 3** Take the IPPBX out of manual mode.
-

Procedure

If end user has voicemail enabled:

- Step 1** Put the IPPBX and the Voicemail server in manual mode.
 - Step 2** Delete the voicemail account of the end user.
 - Step 3** Take the IPPBX and the Voicemail server out of manual mode.
-

Procedure

If the end user is associated with device(s):

- Step 1** Put the IPPBX in manual mode.
 - Step 2** Disassociate the user from the device(s).
 - Step 3** Take the IPPBX out of manual mode.
-

Procedure

If the end user has extension mobility enabled:

- Step 1** Put the IPPBX in manual mode.
- Step 2** Delete extension mobility from CUCDM.
- Step 3** Take the IPPBX out of manual mode.
- Step 4** Delete the device profile from the IPPBX directly.

Note

If multiple steps need to be combined and completed sequentially, then the manual mode needs to be turned on for the first transaction and can be turned off only after the last transaction.

Static Setup of Cisco Unity Connection Manager for LDAP Integration

Cisco Unified Communications Manager (Unified CM) Static Configuration

Procedure

To configure Unified CM for LDAP Integration:

-
- Step 1** Log into the Unified CM for which you want LDAP integration enabled.
- Step 2** Navigate to *System > LDAP > LDAP system*.
- Step 3** Configure the following settings:
- Select Checkbox: Enable Synchronizing from LDAP Server
 - LDAP Server Type: Microsoft Active Directory
 - LDAP Attribute for User ID: sAMAccountName
- Step 4** Navigate to *System > LDAP > LDAP Directory*.
- Step 5** Select the *Add New* option.
- Step 6** Configure the following settings:
- LDAP Configuration Name: *TestLDAP* (use the relevant name)
 - LDAP Manager Distinguished Name: *cn=Administrator,cn=Users,dc=visionoss,dc=int* (use the relevant details)
 - LDAP Password: <password> (password of LDAP server)
 - LDAP User Search Base: *dc=visionoss,dc=int*
 - LDAP Custom Filter: *None*
 - Host Name or IP Address for Server: *1.1.1.1* (ip address or hostname if using DNS of LDAP server)
- Note**
- All other fields should be left as default.
- Step 7** Click the **Save** option.
- Step 8** Navigate to *System > LDAP > LDAP Authentication*.
- Step 9** Configure the following settings:
- Select the checkbox: Use LDAP Authentication for End Users
- Note**
- It should be understood that for the static Unified CM configuration for LDAP integration it is required that the *Use LDAP Authentication for End Users* option be checked because CUCDM does not send passwords to the Unified CM when it is configured as LDAP aware in CUCDM. CUCDM makes the assumption that the Unified CM is LDAP integrated and that Unified CM is configured to use LDAP for authentication of end users.
- LDAP Manager Distinguished Name: *cn=Administrator,cn=Users,dc=visionoss,dc=int* (use the relevant details)
 - LDAP Password: *xxxxxxx* (password of LDAP server)
 - LDAP User Search Base: *dc=visionoss,dc=int* (use the relevant details)
 - Host Name or IP Address for Server: *1.1.1.1* (ip address or hostname if using DNS of LDAP server)
- Step 10** Navigate to *System > LDAP > LDAP Directory*.
- Step 11** Select the previously created LDAP directory.

- Step 12** Select *Perform Full Sync Now*.
- Step 13** Navigate to *User Management >End User*.
- Step 14** Select **Find**.

Verify that LDAP users have been successfully imported into the Unified CM.

Cisco Unity Connection Static Configuration

Procedure

- Step 1** Log into the Cisco Unity Connection server for which you want LDAP integration enabled.
- Step 2** Navigate to *System Settings >LDAP >LDAP Setup*.
- Step 3** Configure the following settings:
- Select the checkbox: *Enable Synchronizing from LDAP Server*
 - LDAP Server Type: *Microsoft Active Directory*
 - LDAP Attribute for User ID: *sAMAccountName*
- Step 4** Navigate to *System Settings > LDAP > LDAP Directory Configuration*.
- Step 5** Select **Add New**.
- Step 6** Configure the following settings:
- LDAP Configuration Name: *TestLDAP* (use the relevant details)
 - LDAP Manager Distinguished Name: *cn=Administrator,cn=Users,dc=visionoss,dc=int* (use the relevant details)
 - LDAP Password: *xxxxxxxx* (password of LDAP server)
 - LDAP User Search Base: *dc=visionoss,dc=int* (use the relevant details)
 - LDAP Custom Filter: *None*
 - Host Name or IP Address for Server: *1.1.1.1* (ip address or hostname if using DNS of LDAP server)
 - LDAP Configuration Name: *TestLDAP* (use the relevant details)
- Note**
- All other fields should be left as default.
- Step 7** Select **Save**.
- Step 8** Navigate to *System Settings > LDAP >LDAP Authentication*.
- Step 9** Configure the following settings:
- Select the checkbox: *Use LDAP Authentication for End Users* (Use the relevant details)

Note

It should be understood that for the static Cisco Unity Connection configuration for LDAP integration it is required that the *Use LDAP Authentication for End Users* option be checked,

because CUCDM does not send passwords to the Cisco Unity Connection when it is configured as LDAP aware in CUCDM. The LDAP authentication should furthermore be configured before performing a full sync with LDAP.

- LDAP Manager Distinguished Name: cn=Administrator,cn=Users,dc=visionoss,dc=int (Use the relevant details)
- LDAP Password: xxxxxxxx (password of LDAP server)
- LDAP User Search Base: dc=visionoss,dc=int (Use the relevant details)
- Host Name or IP Address for Server: 1.1.1.1 (ip address or hostname if using DNS of LDAP server)

Step 10 Navigate to *System Settings > LDAP > LDAP Directory Configuration*.

Step 11 Select the previously created LDAP directory.

Step 12 Select *Perform Full Sync Now*.

Step 13 Navigate to *Users > Import Users*.

Step 14 Find End Users In: *LDAP Directory*.

Step 15 Import With > Based on Template: *voicemailusertemplate*.

Note

CUCDM imports users from LDAP when provisioning voicemail. Transactions will fail if users are already imported to Cisco Unity Connection.

Step 16 Select **users** to import.

Note

If the user does not have a telephone number defined in LDAP, an extension number must be defined before a user can be added. This number can be any value as it changes once the user is added to the system.

Step 17 Navigate to *Users > Users*.

Step 18 Select **Find**.

Verify that LDAP users have been successfully imported into the Cisco Unity Connection.

Cisco Unified Communications Manager IM and Presence (IM and Presence) Server

The system supports the use of IM and Presence servers. A section called *Presence Servers* has been added under the *Network* section. In this section, administrators are able to add, view, configure and delete IM and Presence servers.

Managing a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server

IM and Presence is an enterprise platform that brings people together in and across organizations in the most effective way. This open and extensible platform facilitates the highly secure exchange of availability and instant messaging (IM) information between Cisco Unified Communications and other applications.

To enable IM and Presence server integration, configuration has to be completed in the system as well as on the Server itself.

Procedure

Adding an IM and Presence Server

Step 1 Browse to *Network > Presence Servers*.

Step 2 Click the **Add** button and enter the IM and Presence server details.

The following fields are available when adding an IM and Presence server:

Field	Description
Presence Server Name	Host name for the server. This must be unique in the system and is a mandatory field.
Description	A short description of the server.
Presence Server Publisher IP Address	Specify the IP address for the server. This is a mandatory field.
Software Version	Select the required software version from the drop-down list. This is a mandatory field. Note When migrating to another version of Unified CM, the Software Version must be manually modified to reflect the new Unified CM version.
Admin Username	Specify the user name for configuring the server. This is a mandatory field.
Admin Password	Specify the password for configuring the server. This is a mandatory field.
SIP Destination is a DNS SRV Record	Select this checkbox if the SIP Destination is a DNS SRV Record.
SIP Destinations (Presence Server Hostname or IP Address)	Specify the required SIP destination (Presence Server Host name or IP Address) for SIP Termination. The field can take up to 16 destinations (separated by commas) and each destination can have an optional port stipulate (separated from the destination by a colon); where no port is specified the default port of '5060' will be applied. (Example of 2 destinations and a port specified for the first destination: 10.200.10.102:5070, 10.200.10.103). When the <i>SIP Destination is a DNS SRV Record</i> is selected, only a single destination can be given (without a port), which has to be a hostname. This is a mandatory field.
Manual Mode	Select this checkbox if you would like the server to operate in manual configuration mode. It is mandatory to supply an email address if this option is selected.
Email address	The email address that will be used for manual activation of the server. This field is mandatory if the Manual Configuration Mode? option has been selected.

Step 3 Click the **Add** button.

Note

IM and Presence servers can also be added via the bulk loaders.

Procedure

Connecting an IM and Presence Server to an IPPBX

- Refer to [Connect an IM and Presence Server to an IPPBX on page 607](#).
-

Procedure

Enabling an IM and Presence server on a hardware set to associate with a dial plan

For details on hardware sets and dial plans, see: [Hardware Set Management on page 69](#).

- Step 1** Browse to *Dial Plan Tools > Hardware Sets*.
- Step 2** Select a hardware set.
- Step 3** Enable IM and Presence servers for that hardware set by checking the *UnifiedPresence* checkbox.
- Step 4** Click the **Modify** button. The IM and Presence Server is enabled for the selected hardware set.
-

Procedure

Modifying an IM and Presence Server

To modify an IM and Presence Server:

- Step 1** Browse to the *Network > Presence Servers*.
- Step 2** Select the relevant IM and Presence Server *Name* (active text link).
- Step 3** Modify the required fields then click the **Modify** button. The IM and Presence Server is modified within the system.
-

Procedure

Deleting an IM and Presence Server

To delete an IM and Presence Server from the system:

- Step 1** Browse to the *Network > Presence Servers*.
- Step 2** Click the **Delete** button adjacent to the relevant IM and Presence Server *Name* (active text link). The IM and Presence Server is deleted from the system.
-

Procedure

Testing an IM and Presence Server

To test an IM and Presence Server within the system:

- Step 1** Browse to the *Network > Presence Servers*.

- Step 2** Select the relevant IM and Presence Server *Name* (active text link).
- Step 3** Click the **Test** button. The IM and Presence Server is tested within the system.

Note

The current IM and Presence test functionality within the system is limited to the system querying the version number of the IM and Presence server.

Procedure

Adding IM and Presence to a Feature Group

Note

The task below can also be completed via the bulk loaders.

- Step 1** Browse to *General Administration > Feature Groups*.
- Step 2** Select the appropriate *Feature Group*.
- Step 3** Enable IM and Presence by selecting the *Presence* checkbox in the *Value Add* section of the screen.
- Step 4** Click the **Modify** button. Presence is enabled for the selected feature group.

Procedure

To Configure a User for IM and Presence

Users can also be configured for IM and Presence via the bulk loaders.

Note

- When monitoring a full extension (*All* under the *Device Name* column), all device types for that user that share that extension are monitored (the associated device checkboxes are automatically selected). When adding an extension to another device for the user, the system checks if that extension is fully monitored. If it is, then extension monitoring is automatically enabled for that extension on the device (line instance). If the extension is not fully monitored, then extension monitoring for that line instance is not selected, and the line instance checkbox must be selected manually.
- CUCDM does not currently support IM and Presence Monitoring for cloned lines.
- If the user's Service Profile does not include Presence, a warning is displayed on the screen, 'Warning: User's Service Profile contains no IM and Presence service.'

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** If required, select the customer, division and location. The *User Management* screen is displayed.
- Step 3** Under the *Presence* column, an *Add* link appears if Presence is not configured for that user. If Presence is already configured, a *Y* appears.
- Step 4** Select the *Add* link adjacent to the required user. The *Presence Configuration* screen is displayed.

-
- Step 5** Select the *License User for Unified CM IM And Presence* checkbox - from Presence 9, or the *Enable Presence for User* and *Enable CUPC Capability for User* checkboxes (as appropriate) prior to Presence 9.
- Step 6** Select the *Monitor* checkbox(es) adjacent to the relevant extension(s)/line instance(s) to monitor. The checkbox adjacent to the *Device Name - All* row selects full extension monitoring (including all line instances), and the checkbox adjacent to the individual *Device Type* row selects that specific line instance only for monitoring.
- Step 7** Click the **Apply** button when complete.
-

Connect an IM and Presence Server to an IPPBX

After adding a Cisco Unified Communications Manager IM and Presence (IM and Presence) Server to the system, it can be connected to an IPPBX.

Procedure

Connecting an IM and Presence Server to an IPPBX

Note

The task below can also be completed via the bulk loaders.

To connect an IM and Presence Server to an IPPBX:

- Step 1** Browse to the *Network > Presence Servers*.
- Step 2** Identify the required IM and Presence Server *Name* that you want to connect to an IPPBX.
- Step 3** Click the **Connect to IPPBX** button adjacent to the relevant IM and Presence Server.
- Step 4** Click the **Connect** button adjacent to the relevant IPPBX *Name*.
-

The IM and Presence Server is connected to the IPPBX.

Procedure

Disconnecting an IM and Presence Server to an IPPBX from an IPPBX

Note

An IM and Presence Server cannot be disconnected from an IPPBX if there are users on the IPPBX who have Presence enabled.

To disconnect an IM and Presence Server from an IPPBX:

- Step 1** Browse to the *Network > Presence Servers*.
- Step 2** Identify the required IM and Presence Server *Name* that you want to disconnect from an IPPBX.
- Step 3** Click the **Disconnect from IPPBX** button adjacent to the relevant IM and Presence Server.
-

The IM and Presence Server is disconnected from the IPPBX.

Cisco Unified Communications Manager IM and Presence (IM and Presence) Manual Configuration

Procedure

The IM and Presence server needs the following manual configuration:

Step 1 Initial Post-Install Wizard

- a** Enter the Unified CM Hostname and IP in *Post Install Setup* wizard.

Note

IM and Presence Requires DNS.

- b** Enter *AXL Username* and *Password*, i.e. AXLAdmin and password... (previously created in Unified CM with AXL rights).

Note

This user must have already been created on Unified CM Cluster and is valid - integration fails if not valid.

- c** Enter *Security Passphrase* as it was entered during Unified CM Cluster installation. Entered during system Unified CM Install.

- d** At present , the CallManager Service Parameter Default Inter-Presence Group Subscription needs to be manually set to "Allow Subscription" in order for line presence to function. (This setting is done on Unified CM)

System > Service Parameters > select "server" > Service (Cisco Callmanager) > select "Allow Subscription" drop-down (for Default Inter-Presence Group Subscription).

- e** This is a setting made on Unified CM and can be made at any point during the setup.

- f** Check that Unified CM Publisher Sync status is functional by going to *System > CUCM Publisher*. All four tests should succeed.

Step 2 Add a Presence Gateway for SIP Trunk:

Add Presence Gateway, *Presence > Gateways > Add New* : Enter *Description* and *IP Address* (of Unified CM).

Step 3 Make sure that Automatic Authorization for SIP Clients is enabled to view presence of others:

Presence > Settings, Check *Allow users to view the availability of other users without being prompted for approval*.

Step 4 Enable Legacy Client (CUPC v. 7/8) to download images from Unified CM via TFTP:

Application > Legacy Clients > Settings, Enter *Primary TFTP* (usually Unified CM Publisher) and a Backup TFTP if required.

Step 5 Enable SIP Publish on Unified CM Trunk:

Presence > Settings, and select SIP Trunk created earlier on Unified CM.

Note

Verify SIP Trunk on Unified CM and Presence settings (see under *IM and Presence Service Parameters* in the *Unified CM Build Doc for Cisco Unified Communications Domain Manager*

8.1.2 for details if required). If the server has not been added or connected to a Unified CM in the system yet, the trunk will not yet have been created.

Step 6 Configure Proxy Server Settings

Presence > Routing > Settings, Select *On* (for Method/Event Routing Status), and then *Default SIP Proxy TCP Listener* as Preferred Proxy Server.

Step 7 Allow all SIP via Incoming ACL

System > Security > Incoming ACL, Add New rule with pattern *all*.

Step 8 Activate Presence Services as follows (by logging into Cisco Unified IM and Presence Serviceability > Tools > Service Activation):

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco Sync Agent
- Cisco AXL Web Service

Step 9 Adding VoiceMail, MailStore, Conference, Directory, IM and Presence and CTI Profiles

- This configuration can be done in Unified CM for V9, using UC Services, and a Service Profile applied to a user. See under *Service Profile Management* in the *Deployment Guide* for more details.

Step 10 Add a CCMCIP:

Applications -> Legacy Clients -> CCMCIP Profile.

Optional but recommended for CUPC v.8 users that want to use click to dial. Note that "Cisco Unified Personal Communicator" is now known as "Cisco Jabber Client".

Select the *Make this the default CCMCIP Profile for the system* checkbox and click **Save**.

Step 11 Set the Proxy Domain setting to the enterprise top level domain of the IM and Presence server:

System > Service Parameters > Cisco SIP Proxy > Domain: example.com

Step 12 For the IM and Presence server to accept login requests from CUPC v.7. clients, the following needs to be updated:

Presence > Routing > Method/Event Routing.

- a** Update the Destination Address under *ProfileConfig* to be the FQDN of the IM and Presence server, for example *hostname.example.com*
- b** Update the Destination Address under *SystemPublish* to be the FQDN of the IM and Presence server, for example *hostname.example.com*
- c** Update the Destination Address under *SystemSubscribe* to be the FQDN of the IM and Presence server, for example *hostname.example.com*

Step 13 This step is relevant only when provisioning Unified CM 10.0 (or higher) or when upgrading to Unified CM 10.0 (or higher), and only when LDAP sync has been configured.

A *Home Cluster* checkbox setting was introduced under *User Management > End User* in Unified CM 10.0. This checkbox must be enabled in order for the *Enable User for Unified CM IM and Presence* setting to be available in Unified CM. When LDAP sync has been configured, the *Home Cluster* checkbox is not enabled by default for new Users synchronized from LDAP. In this instance, you must either manually enable the *Home Cluster* checkbox for each User or configure a Feature Group Template on the LDAP synchronization agreement that has *Home Cluster* enabled.

Note

If an administrator configures settings that are managed by the system but via their application admin these settings run a high risk of being erased when the system next provisions these settings. This is due to the system storing configuration information of its own, as domain manager, which is referred to as the master source for user settings. This danger of losing configuration when using application frontends and tools instead of the system features applies to all areas managed by the system. The only exceptions include static configuration task - areas not provisioned by the system.

Driver_Presence Implementation of the *VerifyCUPCapabilities* Transaction

Note

This is applicable only to IM and Presence Version 8.

This transaction verifies that the IM and Presence server and Cisco Jabber Client (changed from Cisco Personal Communicator) capabilities have been propagated to the IM and Presence server from the integrated Cisco Unified Communications Manager (Unified CM). The driver transaction handler reads the capabilities set for the user and matches that to the input parameters for the transaction. The capabilities would have been modified earlier on the Unified CM in the same parent transaction workflow or on a previous transaction.

The verify process can be adapted with the following parameters in the *drivers.conf* file in the */etc/iptcore/* folder. The following variables are available:

- *cups_verify_max_retry*: The *cups_verify_max_retry* setting specifies how many times the user capabilities will be read from the server and verified with the transaction parameters.
- *cups_verify_initial_wait*: The *cups_verify_initial_wait* setting specifies what the initial wait period should be before the first match is attempted
- *cups_verify_interval*: The *cups_verify_interval* setting specifies what wait period to apply between retries.

If the *drivers.conf* file is not present in the */etc/iptcore/* folder, the driver reverts to the following defaults:

- CUPS_VERIFY_DEFAULT_MAX_RETRY: 3
- CUPS_VERIFY_DEFAULT_INITIAL: 0
- CUPS_VERIFY_DEFAULT_INTERVAL: 3

Service Profile Management

Note

Service Profiles are only used and are required by Presence clients at present. The service profile must contain an IM and Presence service, and it is used by the Presence 9 client to define its core and supplementary services.

Service Profiles contain a range of categories (or 'profiles') which are associated with various unified communications services, including Voicemail, MailStore, Conferencing, CTI, Directory, and IM and Presence. Service Profiles are assigned to end users to enable them to access the various services configured in the service profile. Service Profiles are created by adding UC Services to the service profile. UC Services are associated to specific servers which have already

been added to the system. For example, for a service profile to be added and to include an *IM and Presence Profile*, a UC Service of service type *IM and Presence* must first be added to the system. In turn, for the IM and Presence UC Service to be added, a relevant *Presence server* must first be added to the system. The Service Profile can then be associated to an end user.

To facilitate the migration of existing user configurations from Cisco Unified Presence Servers (CUPS) to Cisco Unified Communications Manager (Unified CM), an import functionality has been added to CUCDM to allow a once off import of the UC Services, Service Profiles and the Service Profile associations with end users. (This migration is only possible for Unified CM version 9 and later.) After the initial import, full management of UC Services, Service Profiles and end user associations is provided in CUCDM.

Procedure

Importing Service Profiles from a Cisco Unified Communications Manager (Unified CM)

To import Service Profiles from a Unified CM:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *server* (active text link).
- Step 3** Click the **Import/ Refresh Items** button.
- Step 4** Select the *Service Profiles* checkbox.
- Step 5** Click the **Import/ Refresh Items** button.

Procedure

Viewing / Modifying a Service Profile

To modify a Service Profile:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *server* (active text link).
- Step 3** Click the **Service Profiles** button.

Note

The **Service Profile** button is only displayed when the IPPBX (Unified CM) is version 9.0 or later.

- Step 4** A list of Service Profiles is displayed. The details for each service profile include: Service Profile Names, Service Profile Description, and an indication of whether the service profile is the CUCM Default.

Select the *Service Profile Name* (active text link).

- Step 5** Modify the settings for the service.
- Step 6** Click the **Modify** button.

Note

To view a list of Service Profiles while any Service Profile related screen is displayed, click the **List Service Profile** button. To modify a specific service profile on the displayed list, follow the steps above.

Add UC Service

Procedure

Adding UC Service

To add UC Services:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *server* (active text link).
- Step 3** Click the **Service Profiles** button.
- Step 4** Click the **Add UC Service** button.
- Step 5** Complete the required fields. The fields displayed and the associated data available in the drop-down lists are dynamic and depend on the combination of *Service Type* and *Product Type* selected. Available fields include:

Field	Remarks
Service Type	Select from the drop-down list the UC Service Type, e.g. Voicemail, Mailstore, Conferencing, IM and Presence, and CTI.
Product Type	Select from the drop-down list the Product Type associated with the selected Service Type.
Name	Enter a name for the UC Service. Note The name cannot be 'None'.
Description	Enter a description for the UC Service.
Host Name/ IP Address	The Host Name/ IP Address for the UC Service.
Port	Enter the Port number for the UC Service. An editable default value is displayed.
Protocol	Select from the drop-down list a Protocol for the UC Service.
User web conference server as SSO identity provider	This checkbox will only be displayed when the <i>Service Type</i> is 'Conferencing' and the <i>Product Type</i> is 'WebEx (Conferencing)'. Select the checkbox to define WebEx as the SSO provider.
Connection Type	This drop-down list will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. This field specifies the directory server type to connect to: Global Catalog server that is optimized for searching or a Domain Controller (or any server running an Ldap service) which may not be optimized for searching.
Use Secure Connection	This checkbox will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. Default=selected, which means that credentials will not be sent in clear text.
Use Wildcards	This checkbox will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. Select the checkbox to allow the use of wildcards when doing number lookups.
Disable Secondary Number Lookups	This checkbox will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. Select the checkbox to disable queries from using home, mobile and other numbers.
URI Prefix	This field will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. Specify the URI scheme name e.g. 'im:' or 'sip:'. Maximum length=32.

Field	Remarks
Phone Number Masks	This field will only be displayed when the <i>Service Type</i> is 'Directory' and the <i>Product Type</i> is 'Enhanced Directory'. Allows a mask to be defined which can be used when doing resolution by telephone number. E.g. the mask +353 +(####) ## ## ##### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Multiple masks can be defined by using the ' ' operator. For example: +353 +(####) ## ## ##### +44 +44 (##)## ##### ## ## ##### could be used to resolve numbers in the format +35311221234 to +(353) 11 22 1234. Maximum length=1024.

Step 6 Click the **Add** button.

UC Service Management

Procedure

List/ Modify UC Services

To list/ modify UC Services:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *server* (active text link).
- Step 3** Click the **Service Profiles** button.
- Step 4** Click the **List UC Services** button.

A list of UC Services is displayed. The details for each UC Service include: UC Service Name, UC Service Type, UC Service Product Type, Host/IP Address, Port and Protocol.

To modify a listed UC Service, click the *UC Service Name* (active text link), modify the relevant fields on the next screen and click the **Modify** button.

Note

- The *Service Types* and *Product Types* cannot be modified.
- UC Services cannot be modified via bulk loaders.

Add Service Profile

Procedure

Adding Service Profiles

Note

Due to Cisco Unified Communications Manager (Unified CM) AXL limitations Service Profile parameter values can only be provisioned when there is a Primary UC Service set of that type e.g. the Voicemail parameter "Credentials source for voicemail service" can only be provisioned to Unified CM if a Primary Voicemail Service is included in the Service Profile Add or Modify. Using the Unified CM GUI, these parameters can be saved in the absence of a Primary UC Service. This discrepancy is in the process of being addressed, and CUCDM will support the

saving of these parameters in the absence of a Primary UC Service when the AXL support required is provided.

To add Service Profiles:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the relevant *server* (active text link).
- Step 3** Click the **Service Profiles** button.
- Step 4** Click the **Add Service Profile** button.
- Step 5** Complete the required fields in the *Details* section. Available fields include:

Field	Remarks
Name	Enter a name for the Service Profile. Mandatory field. Note The name cannot be 'None'.
Description	Enter a description for the Service Profile.
Make this the default service profile on CUCM	Select the checkbox to make this the default Service Profile on Unified CM. A default Service Profile is not required, and can be set on only one Service Profile at any given time - by enabling the default checkbox on a Service Profile, the previous default is replaced (this is in keeping with Unified CM functionality.) The Default Service Profile is used by End Users who do not have a Service Profile set.
Voicemail Profile	
Primary	Select a Voicemail UC Service from the drop-down list to serve as primary service for this profile. Note When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.
Secondary	Select a Voicemail UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select a Voicemail UC Service from the drop-down list to serve as tertiary service for this profile.
Credentials source for voicemail service	Select the credentials source for the voicemail service from the drop-down list. If user credentials for the voicemail service are shared with another service, select the appropriate service from this drop-down list. The user credentials automatically synchronize from the service that is selected.
MailStore Profile	

Field	Remarks
Primary	<p>Select a MailStore UC Service from the drop-down list to serve as primary service for this profile.</p> <p>Note</p> <p>When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.</p>
Secondary	Select a MailStore UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select a MailStore UC Service from the drop-down list to serve as tertiary service for this profile.
Inbox Folder	Enter the name of the folder on the MailStore server in which to store new messages. Default value= 'INBOX'.
Trash Folder	Enter the name of the folder on the MailStore server in which to store deleted messages. Default value= 'Deleted Items'.
Polling Interval (in seconds)	The time (in seconds) that can elapse between polls ('checks') of the IMAP server for new voice messages, when IDLE is not supported by the mailstore or when a connection failure occurs. Allowed values: 60 - 900.
Allow dual folder mode	Select the checkbox to allow dual folder mode. This dual folder setting is checked by default for use with mailstores that support the IMAP UIDPLUS extensions (RFC 2359 and 4315). By default, the Client Services Framework (CSF) detects if UIDPLUS is not supported and automatically reverts to Single Folder mode. Deselect this checkbox if UIDPLUS is not supported and the system is to be forced to use Single Folder mode.
Conferencing Profile	
Primary	<p>Select a Conferencing UC Service from the drop-down list to serve as primary service for this profile.</p> <p>Note</p> <p>When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.</p>

Field	Remarks
Secondary	Select a Conferencing UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select a Conferencing UC Service from the drop-down list to serve as tertiary service for this profile.
Server Certificate Verification	Select from the drop-down list the acceptable method of server certificate verification, e.g. 'Any', 'Self Signed or Keystore' or 'Keystore Only'. Default=Any.
Credentials source for web conference service	Select the credentials source for the conference service from the drop-down list. If user credentials for the conference service are shared with another service, select the appropriate service from this drop-down list. The user credentials automatically synchronize from the service that is selected.
Directory Profile	
Primary	<p>Select a Directory UC Service from the drop-down list to serve as primary service for this profile.</p> <p>Note</p> <p>When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.</p>
Secondary	Select a Directory UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select a Directory UC Service from the drop-down list to serve as tertiary service for this profile.
Use UDS for Contact Resolution	User data service (UDS) is a service that provides access to user information stored in the Unified CM backend storage. Select the checkbox to use the UDS service provided in Unified CM for the directory lookup instead of external directory. Default=selected.
Use Logged On User Credential	Anonymous access might be possible on your directory server, but it is not advisable. Select this checkbox to prevent anonymous queries and force the user to enter credentials to sign in to the LDAP server. If this checkbox is not selected, a user should be created with read-only privileges in the same container on the LDAP server that contains your users. That read-only username and password should be configured in the fields below. Default=selected.
Username	Enter the distinguished name for a user ID that is authorized to run queries on the LDAP server, in the format useraccount@domain.com. Cisco Unified Presence uses this name for authenticated bind with the LDAP server. Maximum length=128.

Field	Remarks
Password	Enter the password for the Username that is authorized to run queries on your LDAP server. This is the LDAP bind password for the administrator-level account that was provided in the Username field in the Directory Service Profile. This username and password should have read-only access to the directory, and may be used by clients to perform queries on the LDAP Server. The username/password is only utilized by clients that use Basic Directory Integration, so it doesn't need to be entered for UDS or Advanced Directory Integration. Even for Basic Directory Integration, the username and password are not required when the "Use Logged On User Credential" is checked.
Search Base 1	This field allows a user to narrow his/her Cisco Unified Personal Communicator contact search queries to a certain part of the LDAP directory. Enter the container or directory on the LDAP server where LDAP users have been configured. Example for the search base with Microsoft Active Directory integration: cn=users,DC=EFT-LA,DC=cisco,DC=com. Maximum length=256.
Search Base 2	This field allows a user to narrow his/her Cisco Unified Personal Communicator contact search queries to a certain part of the LDAP directory. Enter the container or directory on the LDAP server where LDAP users have been configured. Example for the search base with Microsoft Active Directory integration: cn=users,DC=EFT-LA,DC=cisco,DC=com. Maximum length=256.
Search Base 3	This field allows a user to narrow his/her Cisco Unified Personal Communicator contact search queries to a certain part of the LDAP directory. Enter the container or directory on the LDAP server where LDAP users have been configured. Example for the search base with Microsoft Active Directory integration: cn=users,DC=EFT-LA,DC=cisco,DC=com. Maximum length=256.
Recursive Search on All Search Bases	Select the checkbox to allow recursive search of the directory, starting at the search base. Recursive search allows for Cisco Unified Personal Communicator contact search queries to search all of the LDAP directory tree from a given search context (search base). This is a common option when searching LDAP. Default=selected.
Search Timeout (seconds)	Enter a value in seconds for a search to timeout. Default=5. Minimum=1. Maximum=30.
Base Filter (Only used for Advance Directory)	Only use this subkey name if the object type that is to be retrieved with queries that are executed against Active Directory is not a user object. If used, the suggested default value is (objectCategory=person). Maximum length=256.
Predictive Search Filter (Only used for Advance Directory)	Only use this subkey name to retrieve results for predictive searches with queries that are executed against Active Directory using a mechanism other than Ambiguous Name Resolution. If used, the suggested default value is (ANR=). Maximum length=256.
IM and Presence Profile	

Field	Remarks
Primary	<p>Select an IM and Presence UC Service from the drop-down list to serve as primary service for this profile.</p> <p>Note</p> <p>When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.</p>
Secondary	Select an IM and Presence UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select an IM and Presence UC Service from the drop-down list to serve as tertiary service for this profile.
CTI Profile	
Primary	<p>Select a CTI UC Service from the drop-down list to serve as primary service for this profile.</p> <p>Note</p> <p>When a <i>Primary</i> service is selected for any of the profiles, the <i>Secondary</i> drop-down list will be enabled, but without the service chosen for the Primary service in its list of services. When the Secondary service is selected for the same profile, the same will happen for the <i>Tertiary</i> drop-down list; it will be enabled, but the list for the Tertiary service will now exclude the services selected for the Primary and the Secondary services. Should the Primary service be changed while the Secondary and Tertiary services are both selected, then both the Secondary and Tertiary services will be reset to 'None' and the drop-down list for the Tertiary service will be disabled. If the Secondary service is changed after the Tertiary service has been selected, the Tertiary service will be set to 'None'.</p>
Secondary	Select a CTI UC Service from the drop-down list to serve as secondary service for this profile.
Tertiary	Select a CTI UC Service from the drop-down list to serve as tertiary service for this profile.

Step 6Click the **Add** button.

UC Central

The system is able to integrate with a number of Unified Communications applications, including UC Central SIP application server. UC Central is an enterprise tool used to deliver voice, web and video conferencing capabilities to users.

The assumption is made that the relevant Cisco Unified Communications Manager (Unified CM) cluster has been configured correctly and that the required Unified CM groups have been created.

Procedure

Integrating UC Central with the system is a multi-step process. The steps in brief, are as follows:

- Step 1** Load Unified CM configuration models with relevant UC Central settings.
- Step 2** Add UC Central to the relevant Dial Plan's hardware set.
- Step 3** Add a UC Central SIP Application Server.
- Step 4** Enable CTI Manager Service on the required Unified CM servers in the Unified CM cluster.
- Step 5** Connect the UC Central Unified Communications server to the Unified CM cluster (PBX) and Unified CM subscriber servers.
- Step 6** Add the CTI Manager Group associated with the Unified CM cluster.
- Step 7** Create the customer.
- Step 8** Copy Feature group from template.
- Step 9** Enable the UC Central and the Single Number Reach features in the customer's Feature Group.
- Step 10** Create the location.
- Step 11** Add the location's Published PSTN Number.
- Step 12** Enable Single Number Reach Support at the location level.
- Step 13** Add an end user at the location level.
- Step 14** Add extension mobility profile or associate a phone to the end user.
- Step 15** Enable one of the end user's extensions to be a UC Central client extension.
- Step 16** The UC Central administrator will then receive a request from the system to activate the user's UC Central functionality. Once the UC Central administrator has sent an activation request to the system, the end user will be able to use the UC Central functionality.
- Step 17** Enable Eventing for UC Central.

These steps are explained in more detail in the following sections:

- Provisioning UC Central
- Enabling a User's extension as a UC Central extension

Provisioning UC Central

Provisioning UC Central is done at the Provider level.

Procedure

To provision UC Central on the system:

- Step 1** Load Cisco Unified Communications Manager configuration models which define and enable the relevant UC Central settings.

For more information on loading UC Central specific models, please refer to the Call Manager Model Guide.
- Step 2** Modify the Hardware set associated with the relevant Dial Plan, to include UC Central in the Hardware set.

Note

To apply your changes above, disassociate (disconnect) the Hardware set from the Dial Plan and then associate (connect) them again. This needs to be done only once when UC Central is enabled on the system.

See also: [Hardware Set Management on page 69](#) for more information on Hardware sets.

Step 3 Add a UC Central Server to the Provider as follows:

- a** Browse to Network > SIP Application Servers.
- b** Click the **Add** button.
- c** Click the **Add** button next to required UC Central in the *Select Product* list.
- d** Provide the relevant server details.
- e** Click the **Add** button.

For more information on *SIP Application servers* , including how to modify and delete them, see [SIP Application Servers on page 138](#).

Step 4 Enable the *CTI Manager Server* on the required Cisco Unified Communications Manager (Unified CM) servers in the Unified CM cluster as follows:

Note

This step can be done for multiple servers in the same cluster.

- a** Browse to Network > PBX Devices.
- b** Select the relevant server *Name* (active text link).
- c** Click the **Servers** button.
- d** Select the relevant CCM server *Name* (active text link).
- e** Select (enable) the *CTI Manager Server* checkbox.
- f** Click the **Modify** button.

Step 5 Connect the UC Central server to the relevant Unified CM cluster as follows:

- a** Browse to Network > PBX Devices.
- b** Click the **Connectivity** button next to the relevant Unified CM cluster on the list.
- c** Click the PBX=>Third Party SIP button.
- d** Click the **Connect** button associated with the relevant UC Central server.
- e** Complete the required fields and click the **Connect** button.

Note

- The first time that the UC Central server is connected to the Unified CM, all the Subscribers in that Unified CM cluster are provisioned for UC Central (if the server has *CTI Manager Server* enabled).
- If a Subscriber is added at a later stage it has to be connected to the UC Central server manually, i.e. it will not be done automatically when the subscriber is added.

For more information on how to connect a Unified CM cluster to a SIP Application server, see [SIP Application Servers on page 138](#).

Manually connect an UC Central server to the new Subscriber in the Unified CM cluster as follows:

- a. Browse to Network > SIP Application Server.
- b. Select the relevant UC Central server.
- c. Click the **Advanced** button.
- d. Click the **Connect** button associated with the Subscriber server which is to be connected to the UC Central server.

Note

- To disconnect a specific Subscriber server, select the **Disconnect** button.
- If a subscriber is removed from the Unified CM cluster to which an UC Central server is connected, the subscriber needs to be disconnected from the UC Central server first.

Step 6 CTI Manager Groups are used to manage the connections between the UC applications and the cluster. Add the *CTI Manager Group* associated with the Unified CM cluster as follows:

- a Browse to Network > PBX Devices.
- b Click the **CTI Manager Group** button associated with the Unified CM cluster.
- c Click the **Add** button.
- d Provide the relevant CTI Manager Group details.
- e Click the **Add** button.

Note

For every CTI Manager Group that gets created an Application User gets created and associated with it. The name and password for the Application user is the same as the name of the CTI Manager Group. The Application User details can be viewed via *Network > PBX Devices*, then selecting the **Application Users** button adjacent to the IPPBX. For more information on Application User including how to add, modify and delete them, please see the *Application Users* section in the Deployment Guide.

For more information on *CTI Manager Groups*, including how to add, modify and delete them, see [Adding a CTI Manager Group on page 89](#), [Adding a CTI Manager Group on page 89](#) and [Modifying a CTI Manager Group on page 90](#).

Step 7 Create a customer and link it to the applicable Hardware Groups (in HCS).

For more information on adding a customer, including customer settings and how to modify and delete it, see [Customer Management on page 700](#).

Step 8 Create a new Feature Group by copying an existing Feature Group (this is an optional step).

For more information on Managing Feature Groups, see [Feature Group Management on page 500](#).

Step 9 Enable the *UC Central* and the *Single Number Reach* features in the customer's *Feature Group*, by following the steps below:

- a** Browse to General Administration > Feature Groups.
- b** Select the required *Feature Group*.

Note

- You may need to browse to the required Customer, etc.
- The relevant Feature Group could be a feature group copied from an existing feature group, as performed in the optional step 8 above.

- c** Enable the *UC Central* and the *Single Number Reach* features.
- d** Click the **Modify** button.

Now single number reach is enabled in the customer's feature group.

Next, ensure that a PSTN published number is enabled for the location and that SNR is enabled after the correct PSTN published number is configured.

Step 10 Create a location.

For more information on adding a location, including prerequisites, settings and how to modify and delete it, see under "Managing Locations" open page 413.

Step 11 Add the relevant location's *Published PSTN Number* as follows:

- a** Browse to General Administration > Locations.
- b** Select the required *Location* (active text link).
- c** Click the **Advanced Mgt** button on the *Location Management* screen.
- d** Click the PSTN Published Number button.
- e** Provide the Published PSTN Number.
- f** Click the **Add** button.

Step 12 Enable *Single Number Reach Support* at the location level as follows:

- a** Browse to General Administration > Locations.
- b** Select the required *Location* (active text link).
- c** Select (enable) the *Single Number Reach Support* checkbox.
- d** Click the **Modify** button

Note

If *Single Number Reach Support* was already enabled, disable it first and click the **Modify** button, before returning to the same screen to re-enable it.

Step 13 Enable Eventing for UC Central as follows:

- a** Browse to Setup Tools > Eventing.
- b** Click the Enable Trigger Level button.
- c** Select the relevant eventing subsystem's *Name* from the drop-down list.
- d** Click the **Next** button.

- e Select the relevant entities from the system's hierarchy to which the eventing subsystem should apply.
- f Click the **Add** button.

For more information on *Eventing* , including how to enable and disable eventing trigger levels, as well as how to view the events available for the eventing subsystem, see the section on Eventing.

Enabling a User's extension as a UC Central extension

Enabling an end user's extension as a UC Central extension is done at the location level.

Pre-requisite

- Before an administrator can enable an extension for UC Central, the end user must either be associated with a registered device or have a Mobility profile and needs to be allocated to a feature group with Single Number Reach and UC Central features enabled.

For information on how to add and manage an end user, see [Managing Users on page 839](#).

Procedure

Enable a user's extension as a UC Central Client extension as follows:

- Step 1** Browse to *Location Administration > End Users* .
- Step 2** Select the required *User* .
- Step 3** Click the **UC Central** button.

Note

The default is *No Extension Selected* if the user has not yet selected an extension to be enabled as a UC Central Client extension.

- Step 4** Select one of the extensions to be enabled as a UC Central Client extension.
- Step 5** Click the **Add** button.

Note

Once the **Add** button has been clicked, the extension is only marked as enabled for UC Central. The actual activation processing only happens when the UC Central administrator sends an activation request to process the UC Central enabled extensions. This is done via API's and not the GUI interface.

Note

- For Self Care, if the user has UC Central enabled in the feature group, the *UC Central* link will be available in the Self Care menu, and the user can enable an extension for UC Central there.
- Existing SNR configuration on the enabled line will be removed and the new SNR configuration will be added.
- Once activated, the user will not be able to make any changes to the UC Central extension.

Disabling a User's extension as a UC Central extension

Procedure

Disable a user's extension as a UC Central Client extension as follows:

- Step 1** Browse to *Location Administration > End Users* .
 - Step 2** Select the required *User* .
 - Step 3** Click the **UC Central** button.
 - Step 4** Select the *Disable UC Central* option.
 - Step 5** Click the **Apply Changes** button.
-

Deactivating a User's UC Central connection

Procedure

Deactivate a user's UC Central connection as follows:

- Step 1** Browse to *Location Administration > End Users* .
 - Step 2** Select the required *User* .
 - Step 3** Click the **UC Central** button.
 - Step 4** Click the **Deactivate** button.
-

Note

When UC Central is deactivated for a user, the extension will remain enabled for UC Central.

For more information on managing a user's UC Central extension, see [UC Central on page 874](#).

Voicemail Services Management

Voicemail services enable the recording and storage of voice messages for end-users when they are either busy or away from their phones. As a Provider Administrator, you will need to configure and manage Voicemail resources for each Customer and as new Locations are added.

See also: [Manage Voicemail Accounts on page 867](#).

Note

- In order for Voicemail accounts to be created for end-users, the services have to be created as a resource by the Provider administrator for each Customer and then created as a Service in each Location.
- Voicemail resources at the Provider level require a Site Code to be created before you can add the Voicemail Resource. The Site Code must be created within the Customer; hence the Voicemail resource is tied to that Customer. The Voicemail Service in effect becomes a special Location within the Customer and E164 numbers can then be moved into the Voicemail Resource.

- Voicemail resource must be allocated a Pilot Number(s). The pilot number is required when a Location Voicemail Service is created to identify it within the Voicemail system. The Pilot Number is used by Users to call the Voicemail system to retrieve messages against their account (i.e. Line) number.

Add a Voicemail Service

Procedure

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Click the **Add** button.
- Step 3** Provide all of the required details. The following fields are available when adding a Voicemail Service (fields available depend on the configuration):

Field	Description
<i>Name</i>	The name of the Voicemail Service being added. The name must be unique, and is a mandatory field.
<i>Description</i>	A short description of the Voicemail Service being added.
<i>Country</i>	The Country within which the Voicemail Service will operate. This is a mandatory field.
<i>Site code</i>	The site code where the Voicemail service will be operating. The Site Code can be a maximum of four (4) digits. This is a mandatory field.
<i>Voicemail Server Hardware Group</i>	The Voicemail server hardware group that the service will utilize. The Voicemail server hardware group must be added before the Voicemail service can be added. This is a mandatory field.
<i>Extension Length</i>	The required extension length for the voicemail service (1 to 11 - select from the drop-down list). This is a mandatory field.
<i>Voicemail PSTN Dial Prefix</i>	The PSTN prefix that will be used to access the Voicemail service. This is a mandatory field.
<i>Visual Voicemail</i>	Select the checkbox to enable the Visual Voicemail feature (if the necessary permissions are configured).

- Step 4** Click the **Add** button when complete. The Voicemail Service is added to the system.

View or Delete a Voicemail Service

Procedure

View and Modify a Voicemail Service

To view and modify a Voicemail Service:

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Select the Voicemail Service *Name* (active text link) of the Voicemail Service that you would like to view.
- Step 3** Modify the required fields. See table under [Add a Voicemail Service](#) on page 625 for a list and brief description of the available fields.

When modifying a voicemail service, the following advanced options are also available:

Option	Accessed via:	Description
<i>Internal Number Management</i>	The Internal Number Mgt button	This function enables you to manage your extensions. Including browsing Internal Numbers, viewing there associated PSTN Numbers and by who/what they are used by.
<i>PSTN Published Number</i>	The PSTN Published Number button	This function enables you to manage your Published PSTN Number. From here you are able to add, delete and modify the related Published PSTN number.
<i>PSTN Number Management</i>	The PSTN Number Mgt button	This function enables you to associate and disassociate PSTN number ranges as well as manage PSTN numbers related to the voicemail service.
<i>Pilot Number</i>	The Pilot Number button	This function enables you to manage the pilot numbers related to the voicemail service. Here you are able to add, modify and delete pilot numbers.
<i>Voicemail Template Management</i>	The Voicemail Template Mgt button	This function enables you to select available voicemail templates for the voicemail service.

- Step 4** Click the **Modify** button. The system updates the relevant details of the selected Voicemail Service.

Procedure

Delete a Voicemail Service

To delete a Voicemail Service:

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Click the **Delete** button. The Voicemail Service is deleted from the system (only if nobody is currently subscribed to the service).
-

Conferencing

This section covers Conference Service Management and WebEx Conferencing

Conference Service Management

In order to provide end-users with conference call functionality, conference services need to be defined.

Before adding a conference service, please take note of the following:

- For a conference service to be offered at the Location level, they must be created at the Provider level and allocated to the Customers' Locations.
- Provider Administrators need to configure and manage conference resources for each Customer and when new Locations are added.
- Before adding conference services, please ensure that Conference servers have been added to the location.

Adding a Conference Service

Procedure

Adding a Conference Service

To add a conference service:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Click the **Add** button.
- Step 3** Select the required server from the drop-down list for the field *Conference Server Type*, and click the **Next** button.

Note

The type of conference server available depends on the conference servers that have been added to the system and could include IPUnity and WebEx conference servers.

- Step 4** Complete all of the required fields, and click the **Next** button.

Note

Adding a conference service is potentially a multi-page process; once you have completed all of the fields on a page, click the **Next** button to proceed to the next page. You can not proceed if a mandatory field is empty.

- Step 5** Once you are confident that all of the fields have been correctly completed, click the **Add** button.

The conference service is added to the system.

The following fields are available when adding an IPUnity conference service:

Field	Description
Name	The name of the conference service being added. This is a mandatory field.
Description	A short description for the conference service.
Country	Country where the conference service is going to be utilized. This is a mandatory field.
Site code	The site code for the conference service. If no site codes are available, you can not add a conference service. This is a mandatory field.
Conference Server Hardware Group	This is a mandatory field. The group within which the conference server is located.
Conference Server	Select the required Conference server from the drop-down list. This is a mandatory field.

Field	Description
Conference Class of Service	The Class of Service is used to define the level and type of functionality provided to users. To configure the conference server's class of service, modify the conference server configuration via the <i>Network > Conferencing Servers</i> menu. This is a mandatory field.
Conference Server Login (email)	The user name used to access the conference server. This does not necessarily need to be an email address, however it is recommended. This is a mandatory field.
Conference Server Password	The password used to access the conference server. This is a mandatory field.
Confirm Server Password	The same password as entered above, repeated here to ensure that the password entered is correct. This is a mandatory field.
Maximum Number of Participants For All parallel reserved conferences	This field specifies the maximum number of participants allowed for all parallel reserved conferences. This number cannot exceed the overall limit configured for the conference server. This is a mandatory field.
Maximum Number of Participants For All parallel Ad hoc conferences	This field specifies the maximum number of participants allowed for all parallel ad hoc conferences. This number cannot exceed the overall limit configured for the conference server. This is a mandatory field.
Maximum Number of Participants per Reserved conference	This field specifies the maximum number of participants allowed per reserved conference. This number cannot exceed the overall limit configured for the conference server. This is a mandatory field.
Maximum Number of Participants per Ad hoc conference	This field specifies the maximum number of participants allowed per ad hoc conference. This number cannot exceed the overall limit configured for the conference server. This is a mandatory field.
Conferencing Option	Select the required conferencing type from the drop-down list. The options are currently <i>audio</i> and <i>audio and web</i> conferencing.

The following fields are available when adding a WebEx conference service:

Field	Description
Name	The name of the conference service being added. This is a mandatory field.
Description	A short optional description for the conference service.
Conference Server	The conference server to be used by this service.
Site Domain Name	<p>This specifies the full site domain name (not the URL), e.g. <i>dummy.webex.com</i>, where <i>dummy</i> represents the site name (unique per customer) and <i>webex.com</i> is the domain name.</p> <p>It must not be prepended with a protocol specifier, e.g. <i>http</i> or <i>https</i>. The system always uses secure <i>http</i> or <i>https</i>.</p> <p>Note</p> <ul style="list-style-type: none"> It is typical for a WebEx site to be used by a single customer, however, the system allows for a WebEx site to be shared by multiple customers. For this reason, the <i>Site Domain Name</i> field is not validated for uniqueness. In shared WebEx scenarios, no partitioning of customers is done on WebEx.

Field	Description
Username	The administrator username to be used by the provisioning interface driver.
Password	The administrator password to be used by the provisioning interface driver. The system password must conform to the minimum WebEx password criteria; if the password does not conform, an error with an indication of why the password does not conform, is displayed after clicking the Add button.
Capacity	This number of users that may be created for the site.
Current Usage	The number of users that have already been created for the site.

Customer administrators can add, modify and delete WebEx services because the network level WebEx entity is required as a placeholder in Unified CM and does not represent any real hardware. The hosted service is fully described for a specific customer at resource level - see: [Provisioning WebEx on page 633](#)

View and Modify a Conference Service

Procedure

Modifying the details of a Conference Service

To modify the details of a conference service:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button to save the modifications.

The conference service is updated within the system.

[PSTN Published Number Management for Conference Services on page 632](#)

Procedure

Modifying a PSTN number of a Conference Service

To modify a PSTN number:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
- Step 3** Click the **PSTN Published Number** button.
- Step 4** Enter the new Published PSTN Number then click the **Modify** button.

Note

It is important to ensure that the correct format is used for this number, otherwise, certain calls to the PSTN (such as those from internal numbers) may fail. The required format is dependent on the configuration of your dial plan, please refer to the *Deployment Guide* for further information.

The conference service is updated within the system.

Procedure

Deleting a PSTN number of a Conference Service

To delete a PSTN number:

- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
 - Step 3** Click the **PSTN Published Number** button.
 - Step 4** Click the **Delete** button.
-

After confirming the delete operation, the PSTN number is deleted.

Procedure

Modifying Internal Numbers related to a Conference Service

Note

This feature is not applicable to a WebEx Conference Service

The Internal Numbers management page consists of a list with three columns, *Internal Number*, *Associated PSTN Number*, and *Used by*.

To modify internal numbers:

- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
 - Step 3** Click the **Internal Numbers Mgt** button.
 - Step 4** To enable an internal number, select the *Allow* active text link, to disable an internal number, select the *Prevent* active text link adjacent to the required internal number.
-

The internal numbers are updated within the system.

Procedure

Modifying PSTN Numbers related to a Conference Service

Note

This feature is not applicable to a WebEx Conference Service

The PSTN number management page consists of a list that displays a list of available lines. The three columns in this list include *DDI Extension*, *Number* and *Used by*.

To modify the PSTN number related to a conference service:

-
- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
 - Step 3** Click the **PSTN Number Mgt** button.
 - Step 4** To modify a line, select the *line name* (active text link).
 - Step 5** After having made the necessary modifications, click the **Modify** button.
-

The conference service is updated within the system.

[Modifying the PSTN to Extension Range Mapping related to a Conference Service on page 631](#)

[Conference Service Pilot Numbers on page 631](#)

Procedure

Deleting a Conference Service

To delete a conference service:

- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the *Name* (active text link) of the conference service that you would like to delete.
 - Step 3** Click the **Delete** button.
-

After confirming the deletion, the conference service is deleted from the system.

Modifying the PSTN to Extension Range Mapping related to a Conference Service

Procedure

Modifying the PSTN to Extension Range Mapping related to a Conference Service

To modify the PSTN to Extension Range Mapping related to a conference service:

- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
 - Step 3** Click the **PSTN Number Mgt** button.
 - Step 4** Click the **Range Assoc** button.
 - Step 5** A list of the current mappings is listed. Make the required modifications and click the **Modify** button.
-

The conference service is updated within the system.

Conference Service Pilot Numbers

Procedure

Modifying Pilot Numbers related to a Conference Service**Note**

This feature is not applicable to a WebEx Conference Service.

To add a Pilot Number to a conference service:

Note

Only **one** pilot number can be added to each conference service.

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
- Step 3** Click the **Pilot Number** button.
- Step 4** Click the **Add** button.
- Step 5** Complete the required fields and click the **Add** button.

The following fields are available:

Field	Description
Pilot Number	The pilot number that you would like to use, this is a mandatory field.
TimeZone	The time zone where the conference service is utilized.

The conference service is updated with the new pilot number.

Procedure

Deleting a Pilot Number related to a Conference Service

To delete a Pilot Number related to a conference service:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
- Step 3** Click the **Pilot Number** button.
- Step 4** Click the **Delete** button adjacent to the pilot number that you would like to delete.

After confirming the deletion, the pilot number is deleted from the system.

PSTN Published Number Management for Conference Services**Procedure**

Modifying the PSTN Published Number of a Conference Service**Note**

This feature is not applicable to a WebEx Conference Service.

To add a PSTN number:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the *Name* (active text link) of the conference service that you would like to modify.
- Step 3** Click the **PSTN Published Number** button.
- Step 4** Enter the required number in the Published PSTN Number field then click the **Add** button.

Note

It is important to ensure that the correct format is used for this number, otherwise, certain calls to the PSTN (such as those from internal numbers) may fail. The required format is dependent on the configuration of your dial plan, please refer to the *Deployment Guide* for further information.

The conference service is updated within the system.

WebEx Conferencing

The system provides functionality to allow end users access to Cisco WebEx conferencing, via the system's interface.

The WebEx solution is remote, meaning that there is no customer specific infrastructure for WebEx. The provisioning of WebEx in the system focuses on creating a virtual infrastructure enabling the end user to access WebEx via the system.

However, this virtual provisioning of the infrastructure follows the normal system requirements and workflow for managing hardware sets, servers and services.

Note

There are no specific dial plan requirements for WebEx as all calls to and from WebEx are completed via the PSTN. The system requires Internet access to connect to WebEx. The https port (443) must be configured to allow Internet access from the system's Server.

Provisioning WebEx

Prerequisites

The WebEx site must already be configured for each customer. WebEx is not provisioned by the system as it is a hosted service. WebEx needs to be configured by the WebEx service team. The exact procedures are provided by the WebEx team, but essentially it involves emailing the WebEx provisioning team the necessary customer details for the site.

Note

To provision Webex for a user, the user must be allocated to a feature group in which the *Conferencing* feature checkbox is selected (enabled) - see [Features Available when Adding or Modifying a Feature Group on page 505](#).

Procedure

To provision WebEx conferencing on the system:

- Step 1** Modify the Hardware set associated with the relevant Dial Plan, to include WebEx in the Hardware set.

Note

To apply your changes above, disassociate (disconnect) the Hardware set from the Dial Plan and then associate (connect) them again.

See also:

- [Hardware Set Management on page 69](#) for more information on Hardware sets.

- Step 2** Add a WebEx Server to the Provider as follows:

- Browse to *Network > Conference Servers*.
- Click the **Add** button.
- Click the **Add** button next to WebEx in the product list.
- Provide the relevant server details. The following fields are available:

Field	Description
Server Name	A system wide unique name for the WebEx server
Description	Optional descriptive information for server
Software Version	A list of supported provisioning interface versions
Manual Configuration Mode? (Use for Un-Managed Clusters)	This allows for enabling of manual mode for all services associated with the WebEx Server. Manual mode simulates successful transactions by the WebEx driver.

- Click the **Add** button.

Note

Connecting a WebEx Conference server to a *transit switch* is not applicable. Therefore, the **Conference Server => Transit Switch** button should *not* be clicked.

Note

The network level entity is required as a placeholder in Unified CM and does not represent any real hardware. The hosted service is fully described for a specific customer at resource level.

- Step 3** Add a WebEx Service to a Customer as follows:

- Browse to *Resources > Conference Services*.
- Click the **Add** button.
- Select the WebEx option from the drop-down list for the field Conference Server Type, and then click the **Next** button.

Note

If IPUnity conferencing is available to the Customer, the IPUnity server is displayed as an option in the *Conference Server Type* drop-down list.

- Provide the relevant service details. The following fields are available:

Field	Description
Name	A unique per customer conference service name

Field	Description
Description	Optional descriptive information for the service
Conference Server	The conference server entity to be used by this service
Site Domain Name	<p>This specifies the full site domain name (not the URL), e.g. dummy.webex.com, where dummy represents the site name (unique per customer) and webex.com is the domain name.</p> <p>It must not be pre-pended with a protocol specifier, e.g. http or https. The system always uses secure http or https.</p> <p>Notes:</p> <p>It is typical for a WebEx site to be used by a single customer, however, the system allows for a WebEx site to be shared by multiple customers. For this reason, the Site Domain Name field is not validated for uniqueness.</p> <p>In shared WebEx scenarios, no partitioning of customers is done on WebEx.</p>
Username	The administrator username to be used by the provisioning interface driver.
Password	<p>The administrator password to be used by the provisioning interface driver.</p> <p>Note: The system password must conform to the minimum WebEx password criteria; if the password does not conform, an error with an indication of why the password does not conform, is displayed after clicking the Add button.</p>
Capacity	This number of users that may be created for the site.
Current Usage	The number of users that have already been created for the site.

- e Click the **Add** button.

Step 4 Add the WebEx service to a customer's Feature Group by selecting the Conferencing option.

Note

See the Feature Group Administration section of this document for more information on Feature Groups.

Step 5 Add the WebEx service to User as follows:

- a Browse to Location Administration > End Users.
- b Select the *Username* (active text link) of the relevant user.
- c Click the **Conference** button on the *User Management* screen.
- d Select the relevant WebEx service option from the drop-down list for the field Conference Service then click the **Next** button.

Note

If IPUnity conferencing is available to the Location, the IPUnity service is displayed as an option in the Conference Service drop-down list.

- e On the next screen, a confirmation of the WebEx service being added for the user is displayed, click the **Add** button.

WebEx is added to the user's profile in the system and the user's details are registered on the WebEx remote service.

The following WebEx fields are set using information available to the system or via static configuration:

Webex Parameter	System Parameter	Fixed
firstName	user/firstName	
lastName	user/lastName	
Title	user/title	
Description	Information	
Company	customer/customerName	
webExId	userName	
Email	emailAddress	
Password	password	
Active		Activated Note When the end user is registered on WebEx, the account status is activated.

With the exception of the user's password, these fields are not updated in WebEx when it is modified in the system (the modifications need to be done separately in WebEx).

Modify a WebEx Service

Procedure

To modify a WebEx Service's details:

- Step 1** Browse to *Resources > Conference Services*.
 - Step 2** Select the required WebEx service *Name* (active text link).
 - Step 3** Modify the available fields.
 - Step 4** Click the **Modify** button. The WebEx service is modified in the system.
-

Delete a WebEx Server

Procedure

To delete a WebEx Server:

- Step 1** Browse to *Network > Conference Servers*.
 - Step 2** Select the required WebEx server *Name* (active text link).
 - Step 3** Click the **Delete** button. The WebEx server is deleted from the system.
-

Delete a WebEx Service

Procedure

To delete a WebEx Service:

- Step 1** Browse to *Resources > Conference Services*.
- Step 2** Select the required WebEx service *Name* (active text link).
- Step 3** Click the **Delete** button. The WebEx service is deleted from the system.

Single Inbox

Single Inbox is a Cisco Unity Connection 8.5 feature that enables users to have a single inbox in their e-mail client that is used for their e-mail as well as their voicemail.

Note

- This feature is only available on Cisco Unity Connection 8.5 and above.
- Users must have email addresses configured for this feature to work. If this feature is activated for a user that does not have an email address provisioned, the system will provision the Single Inbox functionality for the user but it will not be activated.
- The Single Inbox functionality will only be visible to users whose voicemail is provided by a Cisco Unity Connection 8.5 server. The *Unified Messages Service* drop-down list on the *Create Voicemail Account* or *Manage Voicemail Account* screens will not be visible to users who do not have access to the Single Inbox functionality.
- Administrators must manually synchronize the system and the Cisco Unity Connection 8.5 after making changes to the Cisco Unity Connection server. This is done by clicking the **Update Static Config** button on the *Manage Unity Connection Cluster* page, accessed via *Network > Voicemail Servers*.
- In order for a user to successfully use the Single Inbox functionality, they must be created with a Subscriber template that has a Class of Service that is checked with the *Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox* setting.
- The system does not automatically integrate Cisco Unity Connection Servers with Microsoft Exchange, the details for that process can be found here: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/unified_messaging/guide/85xcucumgx.html.

Activating Single Inbox

Note

The system assumes that Single Inbox functionality has been enabled and is correctly configured on the Cisco Unity Connection 8.5 server.

Cisco Unity Connection 8.5 voicemail servers are added in a similar manner to other voicemail servers, by browsing to *Network > Voicemail Servers*. However, after adding the Cisco Unity Connection server, Administrators must manually synchronize the system and the Cisco Unity Connection 8.5. This is done by clicking the **Update Static Config** button on the *Manage Unity Connection Cluster* page, accessed via *Network > Voicemail Servers*.

Once enabled and correctly synced, the *Unified Messages Service* drop-down list will appear under the *Single Inbox* section of the screen on the *Create Voicemail Account* and *Manage Voicemail Account* screens.

Selecting a Unified Messaging Service for Single Inbox

Procedure

When adding voicemail to a user, administrators will be required to select a relevant Unified Messaging Service. To select a Unified Messaging Service:

- Step 1** Browse to *Location Administration > End Users* .
 - Step 2** If requested, select the relevant Provider, Customer, Division and Location.
 - Step 3** Select the *Add* active text link under the *Voicemail* column or select a user then click the **Voicemail** button.
 - Step 4** Select the relevant *Unified Messaging Service* from the drop-down list.
 - Step 5** Click the **Add** button. The user's voicemail will be activated with the single inbox functionality enabled.
-

Modifying the Unified Messaging Service for an Existing Voicemail Account

Procedure

When modifying a user's voicemail account, administrators are able to modify the Unified Messaging Service. To modify the Unified Messaging Service:

- Step 1** Browse to *Location Administration > End Users* .
 - Step 2** If requested, select the relevant Provider, Customer, Division and Location.
 - Step 3** Select the *In Service* active text link under the *Voicemail* column or select a user then click the Voicemail button.
 - Step 4** Select the relevant *Unified Messaging Service* from the drop-down list.
 - Step 5** Click the Modify button. The user's voicemail will be modified with the new Unified Messaging Service.
-

Corporate Directory Partitions

This feature allows an administrator to divide a customer's corporate directory into partitions (or "groups") and to assign customers, divisions, locations or users to those partitions. Only one directory partition can be defined at any and each of these levels. The only place where a directory partition can be created, is at customer level.

The aim is to present a more manageable and more relevant list of phone numbers to an end user, based on the partition to which an end user is assigned.

By default, all administrators have permission to manage the directory partitions for the entities linked to them in the hierarchy. This assignment of a directory partition, to any level other than customer level, is to limit the control that a location, division or customer administrator can have over the partition.

Directory partition can be set at user level, otherwise, the directory partition is inherited from the next higher level (up to customer level). If a user is logged into a phone, the directory partition used to fetch the corporate directory contents is that of the user. Similarly, in the case of a phone

that is associated to a user, that user's directory partition determines what is displayed in the corporate directory. In the case of an un-associated phone with no user logged in, the phone's hierarchy determines the directory partition that will be used. Note that when a phone has no directory partition, the directory partition is also inherited from the next higher level (up to customer level).

With extension mobility enabled, the assumption is currently that the directory partition assigned as per the search pattern above, will follow the user on the phone where they log in, as long as that phone is located within the same customer as the user. Please note that a user has to log in to a phone for extension mobility to work.

Procedure

Add a Directory Partition

To add a directory partition:

- Step 1** Browse to *Setup Tools > Directory Partitions*.
- Step 2** Select the required *Customer* (active text link).
- Step 3** Click the **Add** button.
- Step 4** Complete all of the required fields. The following fields are available:

Field	Remarks
Name	The name of the partition you want to create. The name must be unique for the selected customer.
Description	A free text description for the partition being added.

- Step 5** Click the **Add** button.

Procedure

Modify a Directory Partition

To modify a directory partition:

- Step 1** Browse to *Setup Tools > Directory Partitions*.
- Step 2** Select the required *customer* (active text link).
- Step 3** Select the *partition* (active text link) to modify from the list of partitions available.
- Step 4** Complete all of the required fields. The following fields are available for updating:

Field	Remarks
Description	A free text description for the partition being added.

- Step 5** Click the **Modify** button.

Procedure

Delete a Directory Partition

To delete a directory partition:

- Step 1** Browse to *Setup Tools > Directory Partitions*.
- Step 2** Select the required *customer* (active text link).
- Step 3** Select the *partition* (active text link) to delete from the list of partitions available.
- Step 4** Click the **Delete** button.

Note

A partition can only be deleted if it isn't currently assigned to a user, location, division or customer.

See also: [Assigning a Directory Partition on page 640](#)

Assigning a Directory Partition

Procedure***Assigning a Directory Partition***

To assign a specific administration level to a directory partition:

- Step 1** Browse to one of *General Administration > Locations / Divisions /Customers*.
- Step 2** Select the entity, for example the location, division or customer (active text link), to associate to a partition.
- Step 3** Complete all of the required fields. The following fields are available when assigning a directory partition:

Field	Remarks
Directory Partition	A list box containing a list of partitions available for the customer. It also contains a default partition.

- Step 4** Select a *partition* in the list box to assign to the entity.

Note

- If the 'Default' ('None') partition is selected in case of the entity not being a customer, the partition is inherited from the first available partition assigned to a parent entity up until the customer level.
- If all the administration levels, including the customer, have the 'None' partition assigned, all users for that customer will be visible to each other in the Corporate Directory.

- Step 5** Click the **Modify** button.
-

Hide a Shared line from Corporate Directory

The hide from corporate directory feature allows an administrator or an end user (via Self Care) to hide any *shared line* for a specific user. The hide from corporate directory feature only affects line visibility, not line functionality. If one calls the shared line it reaches all those who share it.

Procedure

To implement this feature:

- Step 1** Enable the feature in the customer's Feature Group as follows:
- a** Browse to General Administration > Feature Groups.
 - b** Select the relevant *Feature Group* (active text link) or add a new Feature Group by clicking the **Add** button).
 - c** Select the Hide Line From Corporate Directory checkbox to enable.
 - d** Click the **Modify** button.
- For more information on Feature Groups, see [Feature Group Management on page 500](#).
- Step 2** Enable the feature in the Feature Display Policy as follows:
- a** Browse to Setup Tools > Feature Display Policies.
 - b** Select the relevant Feature Display Policy *name* (active text link) or add a new Feature Display Policy by clicking the **Add** button.
 - c** Select the *HideFromCorpDir* checkbox to enable.
- For more information on Feature Display Policies, see under [Feature Display Policies on page 434](#).
- Step 3** Enable the feature for the shared line as follows (this is an optional step - the end user can also perform this step in Self Care):
- a** Browse to Location Administration > Phone Management.
 - b** Select the relevant Device *Name* (active text link).
 - c** In the Private line settings for line section, select the *Hide Line From Corporate Directory* checkbox to effect the Hide from Corporate Directory feature for this line.
 - d** Click the **Modify** button. This line is no longer displayed in the Corporate Directory.
- Step 4** Enable the feature in the user's Extension Mobility Profile as follows (this is an optional step - the end user can also perform this step in Self Care):
- a** Browse to Location Administration > End Users.
 - b** Select the relevant *user* (active text link)
 - c** Click on the **Extension Mobility Profile** button.
 - d** In the Private line settings for line section, select the *Hide Line From Corporate Directory* checkbox to effect the Hide from Corporate Directory feature for this line.
 - e** Click the **Modify** button. This line is now not displayed in the Corporate Directory.

CLI Group Management

The purpose of CLI Groups is to allow a group of users to pass a single Calling Line Identity (CLI) number when a call is made to an internal or external destination. This allows groups in a company, for example sales, support, business group, and so on, to control which CLI is presented and ensure return calls go to the correct destination(s). An Administrator is allowed to create or modify Location or Customer level CLI Groups, provided that the administrator is associated with an Access Profile, which allows him or her to add or modify CLI Groups and that the administrator is at the relevant user level, that is Location administrators are not allowed to add customer level CLI Groups.

External Group CLI in the HCS dial plan is implemented by using the Unified CM to add route, translation and transformation patterns.

Procedure

Add a CLI Group

To add a CLI Group:

- Step 1** Browse to *General Administration > CLI Groups*.
- Step 2** Click either the **Add for Customer** button or the **Add for Location** button, depending on the level in the hierarchy for which the CLI Group is configured.

Note

- For administrators at the customer level or above both add buttons are displayed, but for administrators below the level of Customer only the **Add for Location** button is displayed.
- When the **Add for Location** button is clicked, administrators above the location level must select the relevant Location, before the capture screen is displayed.
- When adding an External CLI Group, the models must first be loaded in CUCDM for any of the below transactions to have an effect on Unified CM. That is, the model information for the model name *AddGCLI-External* must be loaded (see Call Manager Model Guide if required). This only needs to happen once.

- Step 3** Complete the required fields. The available fields include:

Field	Description
Manage Customer CLI Groups	
<i>CLI Group Name</i>	A unique name for the CLI Group.
<i>Division</i>	To filter the display of available numbers that can be added to the CLI Group, a Division must first be selected from the drop-down list. Only divisions linked to the Customer are available for selection. When a CLI Group is being added for a location, the relevant Division is pre-selected and the drop-down list is disabled. For a Division administrator the relevant Division is also pre-selected and the drop-down list is disabled.
<i>Location</i>	<p>To filter the display of available numbers that can be added to the CLI Group, select a Location from the drop-down list. Only locations linked to the selected Division are available for selection. When a CLI Group is being added for a location, the relevant Location is pre-selected and the drop-down list is disabled.</p> <p>Note</p> <p>As soon as the Location is selected a list of numbers is displayed in the <i>Extensions</i> list box.</p>
<i>Search</i>	To search for specific extensions, select either the 'Number starts with' or 'Number ends with' option from the drop-down list and enter a relevant digit(s) in the text field to search for. As the search criteria are being entered, the <i>Extensions</i> list box is re-populated with only relevant numbers, based on the search criteria.

Field	Description
<i>Extensions</i>	<p>The extensions available to the selected Location are displayed in a list box. A hundred extensions are displayed per page. The <i>Page</i> drop-down list indicates the current page being displayed. Select from the drop-down list the page to display or navigate between pages by using << or >> (active links).</p> <p>To select extensions for inclusion in the CLI Group, do one of the following:</p> <ul style="list-style-type: none"> Click on specific extensions (single or multiple) displayed in the <i>Extensions</i> list box. To move the selected extensions to the <i>Selected Extensions in the CLI Group</i> list box, click the Add >> button. Click <i>Select page</i> (active text link) - this selects all the extensions displayed on the current page. To move the selected extensions to the <i>Selected Extensions in the CLI Group</i> list box, click the Add >> button. Click the Page >> button - this moves all the available extensions on the current page to the <i>Selected Extensions in the CLI Group</i> list box. Click the All >> button - this moves all the available extensions, including extensions not displayed on the current page to the <i>Selected Extensions in the CLI Group</i> list box.
<i>Selected Extensions in CLI Group</i>	<p>The extensions selected and moved from the <i>Extensions</i> list display in the <i>Selected Extensions in CLI Group</i> list box. The external and internal CLI configurations apply to these extensions.</p> <p>To remove extensions from the list, do one of the following:</p> <ul style="list-style-type: none"> Click on specific extensions (single or multiple) displayed in the <i>Selected Extensions in CLI Group</i> list box. To move the selected extensions back to the <i>Extensions</i> list box, click the << Remove button. Click on <i>Select All</i>. To move the selected extensions back to the <i>Extensions</i> list box, click the << Remove button. Click the << All button - this moves all the extensions to the <i>Extensions</i> list box. <p>Note</p> <p>For a CLI Group being added to a Customer, the administrator has the ability to add numbers from different Divisions and Locations to the same CLI Group. This can be done by moving numbers to the <i>Selected Extensions in CLI Group</i> (as explained above) and then re-selecting another division and location so that the <i>Extensions</i> list box is repopulated with the newly selected location's available numbers. The numbers that are selected and moved from the <i>Extensions</i> list box are added to the already existing list of numbers in the <i>Selected Extensions in CLI Group</i>.</p>
<i>External CLI configuration</i>	
Select the checkbox to enable external CLI configuration. If this field is not enabled all the fields in this section are deactivated.	

Field	Description
<i>Free Text</i>	Select the radio button to allow a number to be entered in the text field. The number supplied here is the external CLI number for the CLI Group. The format of this number entered must follow the format of the numbers presented in the <i>Associated E164</i> drop-down box. The user has to choose between the <i>Free Text</i> option and the <i>Associated E164</i> option, which is described below.
<i>Associated E164</i>	Select the radio button to allow a primary E164 number to be selected from the <i>Location available E164 numbers</i> drop-down list. The user has to choose between the <i>Associated E164</i> option and the <i>Free Text</i> option, which is described above. Note that only primary E164 numbers are available from the drop-down list .
<i>Location Available E164 numbers</i>	Two related drop-down lists are displayed. Select the location from the first drop-down list. Based on this selection the second drop-down list is populated with the available associated E164 numbers for that location. The number selected is the external CLI number for the CLI Group.
Select the checkbox to enable internal CLI configuration. If this field is not enabled all the fields in this section are deactivated.	
<i>Free Text</i>	Select the radio button to allow a number to be entered in the text field. The number supplied here is the internal CLI number for the CLI Group. The user has to choose between the <i>Free Text</i> option and the <i>Extension Number</i> option, which is described below.
<i>Location Primary extensions (optional)</i>	Only available when <i>Free Text</i> is selected. Two related drop-down lists are displayed. Select the location from the first drop-down list. Based on this selection the second drop-down list is populated with the available primary extensions for that location.
<i>Extension Number</i>	Select the radio button to allow a number to be selected from the <i>Location available extension numbers</i> . The user has to choose between the <i>Extension Number</i> option and the <i>Free Text</i> option, which is described above.
<i>Location Available extension numbers</i>	Two related drop-down lists are displayed. Select the location from the first drop-down list. Based on this selection the second drop-down list is populated with the available extension numbers for that location. The number selected is the internal CLI number for the CLI Group.
<i>Number to display for Call Forwarded Calls to PSTN</i>	Select the checkbox to enable and provide the number to display in the text box. Note Number to display for Call Forwarded Calls to PSTN is only available when External CLI configuration is not enabled.

Step 4 Click the **Apply CLI Group Configuration** button.

On clicking the **Apply CLI Group Configuration** button, the following back-end transactions are triggered:

- AddGCLI - this transaction (and the sub-transaction Driver_AddGCLI) uses Unified CM models to add the CLI Group to the CUCDM. For more information on the models refer to the Call Manager Model Guide.
- Driver_IPPBX - this sub-transaction provisions the relevant Unified CM devices with the CLI Group configuration settings.

Procedure

Modify a CLI Group

To modify a CLI Group:

- Step 1** Browse to *General Administration > CLI Groups*.
- Step 2** Click the relevant *CLI Group Name* (active text link).
- Step 3** Complete the required fields.

Note

- For a detailed description of available fields, refer to the *Add a CLI Group* section.
- When a Division administrator is modifying a customer CLI Group, the administrator is not able to:
 - modify numbers associated with other divisions linked to the Customer, for example to remove numbers from the Selected Extensions in CLI Group list associated with other divisions.
 - modify external or internal CLI configurations.
- When a Location administrator is modifying a customer CLI Group, the administrator is not able to:
 - modify numbers associated with other locations linked to the Customer, for example to remove numbers from the Selected Extensions in CLI Group list associated with other locations.
 - modify external or internal CLI configurations.

- Step 4** Click the **Apply CLI Group Configuration** button.

On clicking the **Apply CLI Group Configuration** button, the following back-end transactions are triggered:

- ModGCLI - this transaction uses the Unified CM models to update the CLI Groups on the CUCDM. For more information on the models refer to the Call Manager Model Guide.
- Driver_DelGCLI and Driver_IPPBX - these sub-transactions are triggered to remove the CLI Group from the CUCDM and from the Unified CM.
- Driver_AddGCLI and Driver_IPPBX - these sub-transactions are triggered to add the modified CLI Group to the CUCDM and to the Unified CM.

Procedure

Delete a CLI Group

To delete a CLI Group:

- Step 1** Browse to *General Administration > CLI Groups*.
- Step 2** Click the relevant *CLI Group Name* (active text link).
- Step 3** Click the **Delete CLI Group Configuration** button.

On clicking the **Delete CLI Group Configuration** button, the following back-end transactions are triggered:

- DelGCLI - this transaction uses the Unified CM models to update the CLI Groups on the CUCDM. For more information on the models refer to the Call Manager Model Guide.
- Driver_DelGCLI and Driver_IPPBX - these sub-transactions are triggered to remove the CLI Group from the CUCDM and from the Unified CM.

Note

Division and Location administrators are not able to delete a customer CLI Group.

Bulk Loading CLI Groups

Bulk loading of CLI Groups is done by loading the *Add CLI Group* sheet (in the LocAdmin sample workbook).

For more information on bulk loading, refer to the Bulk Loader Guide.

Codecs

Codecs determine the data rate for inter and intra region communication. The regions are provisioned on Cisco Unified Communications Domain Manager (CUCDM) and are linked to locations and devices in the system.

Codecs can be set at different levels in the system, namely at dial plan, customer, building, location, and device level (by way of the device pool associated with the device).

When adding a dial plan to the system the user is required to add the codecs for the dial plan. The *Intra-Region Max Audio Bit Rate* and the *Inter-Region Max Audio Bit Rate* are specified separately. These codecs specified in the dial plan are the codecs that apply to the customers, buildings and locations linked to the dial plan.

However, if the *Customer / Building Codec Configurable?* field is selected in the dial plan, then it provides customers, buildings and locations with the option to select their own codecs, thereby over-riding the codecs settings in the dial plan.

When new customers, buildings and locations are added to the system, the codecs fields are available as optional fields to set.

If the admin user chooses not to set inter and intra region codecs to be used for a location (i.e. selects 'None' from the drop-down list), then the setting from the customer will apply. If the customer codec has not been set then the codec from the dial plan (not an optional setting when adding a dial plan) will apply. The location is also able to select the Unified CM default codec setting to over-ride the customer and dial plan settings.

In case a building exists in the hierarchy and the codecs were not selected at location level, then the location will inherit the building's codecs (if it was set) and the building will inherit the customer's codecs (if it was set), otherwise the dial plan's codecs will apply.

The ability to specify codecs per device (indirectly through the specification of a region associated to a device pool) allows administrators to use custom codecs for each device or group of devices at the location level. This builds upon the previous release (Codecs per Location), and allows administrators to specify codecs at the device level. In other words, a hybrid of the two codecs provisioning schemes can be employed.

This new functionality enables Administrators, through the use of multiple device pools, to group devices within a location to allow newer devices to take advantage of higher bit rates, while

allowing older devices to remain on lower bit rates. Previously, the lowest common supported bit rate would have had to be used for an entire customer or location (depending on the configuration used).

Note

The codecs can be set while adding new dial plans, customers, buildings and locations, but they can only be modified via operations tools (for dial plans, customers and buildings) or via administration tools (for locations).

Default Cisco Unified Communications Manager (Unified CM) Codec Values

Unified CM codecs are imported during the *Import / Refresh items* call to Unified CM. Codec selection checks upfront whether or not the set of codecs to be provisioned for a region are equal to those of the default regions. In such cases, no region matrix entry will be created.

For example, if Region A (to be provisioned) has a codec set of 64|8 and the default codecs set up on Unified CM are 64|8, no region matrix entry will be created for region A to itself. Furthermore, any region (including the trunk region) to which region A must be mapped, having default codecs, will result in no mapping operation being called.

The order of operations is therefore the following:

1. Setting the codecs for the location is provisioned via the the system's GUI.
2. The system checks whether the intra-region codecs for the new location are equal to those of the default. If they are the same nothing is done; if they are not the same, the intra-region codec is provisioned.
3. The system checks all regions to which the new region is to be mapped (Location and Trunk) and determines the highest possible combination of codecs.
4. The system checks whether the default inter-region codec matches the newly calculated inter-region codec. If they match, the old region is removed; if they don't match, the new codec is provisioned by creating a matrix entry or updating the old region.
 - See [Dial Plan Management on page 54](#) for more information on setting codecs for dial plans.
 - See [Customer Management on page 700](#) for more information on setting codecs for customers.
 - See [Adding a Building on page 723](#) for more information on setting codecs for buildings.
 - See [Add Location - Page 3 on page 753](#) for more information on setting codecs for locations.
 - See [Operations Tools on page 515](#) for more information on modifying codecs for dial plans, customers or buildings.
 - See [Location Administration Tools on page 821](#) for more information on modifying codecs for locations.

Audio Regions

To specify codecs for a device, the device must be configured to use a device pool.

Regions are manually added via Cisco Unified Communications Domain Manager (CUCDM), and the devices are then configured to use these regions via Location Administration.

Procedure

Managing Audio Regions

To manage regions:

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the *Name* (active text link) of the server that you would like to manage.
- Step 3** Click the **Audio Regions** button. The *Audio Regions* screen is displayed.

This screen allows you to view all the existing custom regions, showing the bandwidths (both inter and intra-region audio).

Regions can be added by clicking the **Add** button, deleted by selecting the checkboxes next to the required Region name and clicking the **Delete Selected** button (for multiple deletions), or simply by clicking on the **Delete** button to the right of the specific region that you want to delete - see *Adding an Audio Region* below.

Caveats

Regions may not be added with the following reserved names:

- "phone-" (for locations where custom regions are not used, a region for the location's phones is created using this key word)
- "Trunk" (regions configured as part of the creation of trunks contain this key word)
- Global Setting for "Global Phone Region", e.g. "GlobalPhonesRegion-"
- Global Setting for "Global Customer Region", e.g. "GlobalCustomerRegion-"
- Global Setting for "Global Building Region", e.g. "GlobalBuildingRegion-"

Existing regions can also be modified - see [Modifying an Audio Region on page 649](#).

See also: [Device Pool Templates on page 558](#) for information on how to assign codecs per device using device pool templates and device pools.

Adding an Audio Region

Procedure

Note

>See also "caveats" when adding an audio region under [Audio Regions on page 647](#)

To add a new audio region:

- Step 1** Click the **Add** button on the *Audio Regions* screen (if required):
- Step 2** Complete the required fields (see table below), and click the **Add** button when complete:

Field	Description
Region Name	This is a mandatory field.
Description	A description to further describe and identify the region name.
Intra-Location Max Audio Bit Rate	Select the required bandwidth from the drop-down list.
Inter-Location Max Audio Bit Rate	Select the required bandwidth from the drop-down list.

Field	Description
Use this codec where possible for mappings	The status of this checkbox determines if the inter-region codecs of the enabled region are used when mapping to either a non-custom region, or to a custom region that does not have the mapping setting enabled. Checkbox selected = enabled. If enabled, this setting effectively disables codec scaling and sets the bandwidth to always use the selected region's inter-region bit rate, even if the region has a higher bit rate than the regions it is mapped to.

Note

When adding a region that exists in Unified CM, the details of the added region are updated with the settings specified.

Bulk Loading Audio Regions

Audio regions can be bulk loaded into the system using the *Add CCM Audio Region* sheet in the *Network* spreadsheet.

For more information on bulk loading audio regions, please see the Bulk Loader Guide.

Modifying an Audio Region

Procedure

To modify an existing audio region:

- Step 1** Select the *Region name* (active text link) of the audio region that you want to modify.
- Step 2** Modify the required fields (see field descriptions under [Adding an Audio Region on page 648](#) if required), and click the **Modify** button when complete.

Bulk Loading Codecs

Intra-region and inter-region codecs can be bulk loaded for dial plans, customers, buildings and locations, using the *Intra-Location Max Audio Bit Rate* and *Inter-Location Max Audio Bit Rate* columns in the loaders for *Add Number Construction* (mandatory fields), *Add Customers* (optional fields), *Add Buildings* (optional fields) and *Add Locations* (optional fields).

If data is not set on the columns for the Add Location codecs then the customer or dialplan codecs will be used. However, these settings will only be set on the location if the customer has the "Location Codec Configurable" set to true and the dialplan has the "Customer Codec Configurable" set to true. These fields are not mandatory.

If the configurable option has been set to true, but no values have been added to the loader then the defaults from the dial plan will be used.

For more information on bulk loading codecs, please see the Bulk Loader Guide.

Automatic Codec Scaling

It is possible that different locations will have different codecs values set. When a call is made between locations the system has to apply the correct codec selection for a location based on the codecs already configured at other locations.

Example:

First Location A is created with: Intra-Region Codec = 64KB

Inter-Region Codec = 8KB

Location	A	B	C
A	64		
B			
C			

Then Location B is created with: Intra-Region Codec = 64KB

Inter-Region Codec = 32KB

Location	A	B	C
A	64		
B	8	64	
C			

New Implementation of codecs (shown above)

Location	A	B	C
A	64		
B	32	64	
C			

Previous Implementation of codecs (shown above)

In the previous implementation of codecs, the mapping between Location A and Location B would have been overwritten with the last location's addition (i.e 32KB). With the new implementation of codecs the system will choose the correct codec that two locations can use to communicate, i.e the lesser of the two and provision that one. Even though the user specified a higher inter-region codec for Location B, it can only communicate with Location A at 8KB.

Then Location C is created with: Intra-Region Codec = 64KB

Inter-Region Codec = 256KB

Location	A	B	C
A	64		
B	8	64	
C	8	32	64

Finally, if we provision Location C, only 8KB can be used between Location A and Location C as 8 is the highest Location A can use and similarly for Location C to Location B.

Contact Centers

This section covers Contact Server Servers and Services.

Contact Center Servers

The system can provision Contact Center integration, specifically for Unified Contact Center Enterprise (Unified CCE) V8.5(1). This integration includes initial connection steps for Cisco Unified Communications Manager (Unified CM) / Unified CCE integration, as well as settings on the User and Phone pages for establishing agents and their phones for the Unified CM.

The feature works in a similar way to Voicemail - in the way that it connects the Contact Center Server, then the Contact Center Service, followed by pilot numbers, and E164 management.

The system only provisions the Unified CM with the necessary dial plan components, JTAPI users and device association. It also provisions transit devices and local gateways with dial plan components to route PSTN numbers. However no provisioning is performed on the Unified CCE server itself.

Procedure

The steps to establish a contact center server are:

- Step 1** First add a contact center server to the system, to identify VRU and transfer/conference patterns.
- Step 2** Connect the Contact Center Server to a Unified CM, to establish a one-to-one relationship and identify the Unified CM server to be used to provision the JTAPI user and routing components for the VRU and conference/transfer numbers.
- Step 3** Create a Contact Center Service to define pilot numbers, external number mappings and to make the service customer specific.
- Step 4** Enable phones and user lines as agent lines. The devices are then associated with the JTAPI user.
- Step 5** If external pilot numbers are to be routed through a location's local gateway, an additional step is needed to associate the Contact Center service to a location, and complete the external number mapping at the location level. (This only applies to locations with activated local gateways.)

Add a Contact Center Server

Procedure

To add a Contact Center Server:

- Step 1** Browse to *Network > Contact Center Servers*.
- Step 2** Click the **Add** button. Mandatory fields include:

Field	Remarks
Host Name	The host name of the Contact Center.
Description	A short description of the server.
Contact Center Version	The drop-down list contains the different Contact Center Versions that are available.
IP Address	Enter the IP of the Contact Center Server.
Country Code	This field allows for the selection of a country code.
CPID	Select the CPID to be used. It defaults to 'auto'.
UCCE Network VRU	A unique VRU pattern. A suffix (..) is added to this field.
Conference/Transfer Route Point Pattern	Deselect the <i>Use default</i> checkbox to be able to enter a value. The default value is '8XXXX'.
Manual mode	Select the checkbox if you would like the SIP Application server to be in manual mode. Note For some SIP Application servers (e.g. Contact Center) manual mode is always pre-selected.

- Step 3** Click the **Save** button.
-

Modify and Delete a Contact Center Server

Procedure

To modify a Contact Center Server:

- Step 1** Browse to *Network > Contact Center Servers*.
- Step 2** Select the required *Contact Center* (active text link).
- Step 3** Make the required modifications, and then click the **Modify** button.
-

Procedure

To delete a Contact Center Server:

- Step 1** Browse to *Network > Contact Center Servers* Server.
- Step 2** Select the required *Contact Center Server* (active text link).
- Step 3** Click the **Delete** button to remove the Contact Center Server.
-

Connecting a Contact Center Server to PBX/Transit

This feature allows a user to connect a Contact Center Server to the PBX/Transit.

This functionality is accessed by browsing to *Network > Contact Center Servers*.

Note

- The Route List: RL-UCCE-CVP-OR-CUBESP-#CCCPID#, (where #CCCPID# is the CPID of the Contact Center Server) must be manually added to the Unified CM before connecting the Contact Center to IPPBX.
 - The Device Pool: GL-DP-CC must be manually added to the Unified CM before connecting the Contact Center to the IPPBX.
 - The Route List and Device Pool names are customized as per the 01 Leaf Cluster Model workbook.
 - Once a Contact Center has been created there are two ways it can be connected to a PBX/Transit device:
-

Procedure

Scenario 1:

- Step 1** Browse to *Network > Contact Center* Server.
- Step 2** Click the **Connectivity** button next to the relevant Contact Center Server.
- Step 3** Click the **Connect** or **Disconnect** button next to the PBX/Transit to connect/disconnect this Contact Center Server.
-

Procedure

Scenario 2:

- Step 1** Browse to *Network > PBX Devices*.
 - Step 2** Click the **Connectivity** button next to the PBX to connect a Contact Center Server.
 - Step 3** Click the **PBX=>Contact Center** button.
 - Step 4** Click the **Connect** or **Disconnect** button next to the PBX/Transit to connect/disconnect the Contact Center Server.
-

Connecting a Contact Center Server to a Hardware Group

This feature allows a user to connect a Contact Center Server to Hardware Group.

This functionality is accessed by browsing to *Network > Hardware Group*.

Creating a Hardware Group for connecting a Contact Center Server

Procedure

To add Hardware Group for connecting to a Contact Center Server:

- Step 1** Browse to *Network > Hardware Groups*.
 - Step 2** Click the **Add** button.
 - Step 3** Select 'Adding Contact Center resources' or 'Any Action' from the Limit usage of this Hardware Group to drop-down list.
 - Step 4** Click the **Next** button.
 - Step 5** The Available Contact Center Servers section is now available for selection. Select the checkbox next to the Contact Center Server to connect the Hardware Group.
 - Step 6** Click the **Add** button.
-

Removing a Hardware Group connected to a Contact Center Server

Procedure

- Step 1** Browse to *Network > Hardware Groups*.
 - Step 2** Select the required Hardware *Group* (active text link).
 - Step 3** Click the **Delete** button.
-

Associating a Customer with a Contact Center Hardware Group

This feature allows a user to associate and disassociate a Hardware Group with a customer.

This functionality is accessed by browsing to *General Administration > Customers*.

Associating a Customer with a Contact Center Hardware Group

Procedure

- Step 1** Browse to *General Administration > Customers*.
 - Step 2** Click the **Advanced Mgt** button.
 - Step 3** Click the **Hardware Group Association** button.
 - Step 4** Click the **Associate** button next to the Hardware Group.
-

Disassociating a Customer from a Contact Center Hardware Group

Procedure

- Step 1** Browse to *General Administration > Customers*.
 - Step 2** Click the **Advanced Mgt** button.
 - Step 3** Click the **Hardware Group Association** button.
 - Step 4** Click the **Disassociate** button next to the Hardware Group.
-

Contact Center Service Management

Contact Centers enable the intelligent routing of all contacts, call treatment, and general contact management over a multi channel IP infrastructure.

This feature allows a user to add, modify and delete a Contact Center Service.

This functionality is accessed by browsing to *Resources > Contact Center Service*.

Adding a Contact Center Service

Procedure

To add a Contact Center Service:

- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Click the **Add** button. Mandatory fields include:

Field	Remarks
Name	The name of the Contact Center Service.
Description	A brief description of the Contact Center Service.
Country	Select a country in which the service is to be provided.
Site Code	Enter the Site Code for the Contact Center Service.
Contact Center Hardware Group	Select a Hardware Group for the Contact Center Service.
Extension Length	Select the Extension Length. It defaults to '3'.

- Step 3** Click the **Next** button.
- Step 4** Select from the drop-down list the *Contact Center Server* to be used for this service.
- Step 5** Enter an appropriate *Extension Range* for this service.

Note

Once an Extension Range is entered these numbers will be generated dynamically.

-
- Step 6** Click the **Add** button.
-

Modifying a Contact Center Service

Procedure

To modify a Contact Center Service:

- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Select the required Contact Center *Service* (active text link).
- Step 3** Click any of the buttons on the top of the screen to modify that specific section for this Contact Center Service, namely:
- Internal Number Mgt
 - PSTN Published Number
 - PSTN Number Mgt
 - Pilot Number
-

Procedure

To delete a Contact Center Service:

- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Select the required Contact Center *Service* (active text link).
- Step 3** Click the **Delete** button.
-

Note

A Contact Center Service can only be deleted if there are no pilot numbers for this service and it is not selected for use at a Location.

Internal Number Management

Extensions are managed by using ranges. Ranges can be added and deleted via two methods:

Procedure

Method 1

- Step 1** Enter the start extension and end extension number or range size.
- Step 2** Click the **Add** or **Delete** range button.
-

Procedure

Method 2

- Step 1** Enter a list of start extension and end extension numbers in a range style. For example, 0000-0100, 0200-0299 etc.
- Step 2** Click the **Add** or **Delete** range button.
-

PSTN Published Number

Procedure

To add a PSTN Published Number:

- Step 1** Click the **Add** button.
- Step 2** Enter the Published PSTN Number.
- Step 3** Click the **Add** button.
-

Contact Center Service External Number Management

Procedure

Associating a PSTN Number Range

To associate a number range:

- Step 1** Click the **Associate Range** button.
- Step 2** The drop-down list displays all the area codes available for numbers in this location. Select the area code for the range you want to associate and click the **Next** button.
- Step 3** Select the relevant range of PSTN numbers and internal extensions and click the **Submit** button.
-

Note: Depending on whether you would like to work with multiple or single extensions, select either the *Map a PSTN Range to multiple extensions* or *Map a PSTN Range to a single extension* section.

Fields	Description	Description
<i>PSTN Number - Range Start</i>	The first E164 number in the range to associate.	Select from the drop-down list. Default = first number in list. The list displays the PSTN numbers of the chosen area code which are not yet associated with an internal extension.
<i>PSTN Number - Range End</i>	The last E164 number in the range to associate.	Select from the drop-down list. Default = first number in list. The list displays the PSTN numbers of the chosen area code which are not yet associated with an internal extension. It is possible to select a range of 1 number.
<i>Extension Number - Range Start</i>	The first internal number in the range to associate.	Select from the drop-down list. Default = first number in list. The list displays the internal extensions which are available in the location and not yet associated with any PSTN number.

Fields	Description	Description
<i>Extension Number - Range End</i>	The last internal number in the range to associate.	Select from the drop-down list. Default = Auto. Auto means that the system associates the available internal extensions sequentially starting from the first extension in the range.
<i>Keep Current Primary E164</i>	Select this checkbox if you would like to use the current Primary E164.	This option is only available if single extensions are being mapped.
<i>Assign New Primary E164</i>	Select this checkbox if you would like to specify a new Primary E164.	Select the new number from the adjacent drop-down list. This option is only available if single extensions are being mapped.

Procedure

Disassociating a PSTN Number Range

To disassociate a number range:

- Step 1** Click the **Disassociate Range** button.
- Step 2** The drop-down list displays all the area codes available. Select the area code for the range you want to disassociate and click the **Next** button.
- Step 3** Select the relevant range of PSTN numbers for disassociation and click the **Remove Association** button.

Note: The system does not allow disassociation of numbers in use, for example numbers which are allocated to users or phones, numbers used as pilot etc.

Available fields include:

Fields	Description	Description
<i>PSTN Number - Range Start</i>	The first E164 number in the range to disassociate.	Select from the drop-down list. Default = first number in list. The list displays the PSTN numbers of the chosen area code which are associated with an internal extension.
<i>PSTN Number - Range End</i>	The last E164 number in the range to disassociate.	Select from the drop-down list. Default = first number in the list. The list displays the PSTN numbers of the chosen area code which are associated with an internal extension. It is possible to select a range of 1 number.

Procedure

Managing Primary E164 numbers

To manage Primary E164:

- Step 1** Click the **Manage Primary E164** button.
- Step 2** Select the relevant values from the drop-down list.

- Step 3** Click the **Submit** button.
-

Pilot Number

Procedure

- Step 1** Click the **Add** button.
- Step 2** Select the Pilot Number from the drop-down list containing extension numbers available from the contact center internal number inventory.
- Step 3** Click the **Submit** button.
-

Add a Pilot number for a Contact Center Service

A pilot number is the address or location of a hunt group within a PBX or IP-PBX and is generally defined as a blank extension number or an extension from a hunt group that does not have a person or telephone associated with it. When using single hunt group or multiple hunt group functionality, each hunt group must be associated a pilot number.

Procedure

Follow these steps to assign a Pilot Number to a Contact Center Service:

- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Select the **Name** (Active text link) of the Contact Center that you would like to assign a Pilot Number to.
- Step 3** Click the **Add Pilot Number** button.
- Step 4** Complete the required fields and click the **Add** button.
-

The Contact Center service is updated with the new pilot number

Available fields include:

Field	Description
<i>Pilot Number</i>	The pilot number that you wish to use for the Contact Center service. This must conform to the standard E164 number format and is a mandatory field.
<i>Description</i>	A short description for the Pilot Number you are adding.

Managing Contact Center Service Pilot Numbers

A pilot number is the address or location of a hunt group within a PBX or IP-PBX and is generally defined as a blank extension number or an extension from a hunt group that does not have a person or telephone associated with it. When using single hunt group or multiple hunt group functionality, each hunt group must be associated a pilot number.

Procedure

Assigning a Pilot Number to a Contact Center Service

Follow these steps to assign a Pilot Number to a Contact Center Service:

-
- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Select the *Name*(active text link) of the Contact Center that you would like to assign a Pilot Number to.
- Step 3** Click the **Add Pilot Number**button.
- Step 4** Complete the required fields and click the **Add**button.
-

The Contact Center service is updated with the new pilot number.

Available fields include:

Fields	Description
<i>Pilot Number</i>	The pilot number that you wish to use for the Contact Center service. This must conform to the standard E164 number format and is a mandatory field.
<i>Description</i>	A short description for the Pilot Number you are adding.

Procedure

Modifying a Pilot Number

Follow these steps to modify a Pilot Number assigned to a Contact Center service:

- Step 1** Browse to *Resources > Contact Center Service*
- Step 2** Select the **Name**(Active text link) of the Contact Center that you would like to modify the Pilot Number for
- Step 3** Select the **Pilot Number**that you would like to modify
- Step 4** Modify the required fields and select the **Modify**button
-

Procedure

Deleting a Pilot Number

Follow these steps to delete a Pilot Number from a Contact Center service:

- Step 1** Browse to *Resources > Contact Center Service*.
- Step 2** Select the *Name*(active text link) of the Contact Center that you would like to delete the Pilot Number from.
- Step 3** Click the **Pilot Number**that you would like to delete.
-

After confirming the operation, the pilot number is deleted from the Contact Center service.

Contact Center Service Location Management

This feature allows a user to add, modify and delete a Contact Center Service at a Location.

This functionality is accessed by browsing to *General Administration > Location*.

Procedure

Associating a Contact Center Service to a Location

To associate a Contact Center Service to a location:

- Step 1** Browse to *General Administration > Location* .
- Step 2** Select the required *Location* (active text link).
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **Contact Center** button. Mandatory fields include:

Field	Remarks
Name	The name of the Contact Center Service for this Location.
Contact Center Service	This field contains a selection of Contact Center Services that are available for the current Location.
Contact Center Pilot Number	Select the Pilot Number for this service.

- Step 5** Click the **Next** button.
- Step 6** Select the *Contact Center Pilot Number* from the drop-down list.
- Step 7** Click the **Add** button.

Note

Only one Contact Center Service is allowed per location. The details screen of the associated service will be displayed if another service is attempted to be added to the location.

Procedure

Associating an Extension Range to a Contact Center Service at a Location

This allows the mapping of an Extension Range to a Contact Center Service at a Location. The functionality is accessed by browsing to *General Administration > Location > Advanced Mgt > Contact Center*.

To associate an Extension Range to a Contact Center Service at a Location:

- Step 1** Browse to *General Administration > Location*.
- Step 2** Select the required *Location* (active text link).
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **Contact Center** button.
- Step 5** Click the **Associate Range** button.

Procedure

Removing a Contact Center Service at a Location

To remove an associated Contact Center Service to a Location:

- Step 1** Browse to *General Administration > Location*.

- Step 2** Select the required *Location* (active text link).
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **Contact Center** button.
- Step 5** Click the **Delete** button.

Associating an Agent Line to a phone / extension mobility profile

Once a contact center server has been created and connected to an IPPBX, it is possible to add the "Contact Center Agent Line" phone feature to a device or extension mobility profile. If the feature group for the device / mobility profile has the "Contact Center Agent Line" feature enabled and the line is not a cloned or shared line, a checkbox will display when managing a phone.

If the line is a shared line or a cloned line, the checkbox will be disabled and an error message will be displayed next to the box.

Marking the checkbox triggers the association of the phone to the JTAPI user when the phone updates are saved. Deselecting the checkbox removes the JTAPI user association when it is the last line left on a phone / mobility profile.

The same workflow applies to extension mobility profiles, i.e. the JTAPI user will be associated to the device profile for extension mobility.

Recording Profiles and Recording Options

Importing of Recording Profiles

To be able to select a Recording Profile it must first be imported from the Cisco Unified Communications Manager (Unified CM).

Procedure

- Step 1** Browse to *Network > PBX Devices*.
- Step 2** Select the required PBX.
- Step 3** Click the **Import/Refresh Items** button.
- Step 4** Select the *Recording Profiles* checkbox.
- Step 5** Click the **Import/Refresh** button.

Note

All available recording profiles are imported and appear under the Phone Management page (see following section on setting the Recording Profile). If a duplicate Recording Profile exists then it updates it with the profile being imported. Should a previous profile exist that is not on the Unified CM it removes that profile from the system.

Setting the Recording Profiles and Recording Options on a Contact Center line

To change the Recording Profile or the Recording Option on a Contact Center enabled line the Agent Line checkbox must be active and checked (as discussed in the previous section). Both these options must be enabled in the Feature Display Policy as well as the Feature Group. These fields are set on a per line basis.

Procedure

To set the Recording Profiles and Recording Options:

- Step 1** Browse to *Location Administration > Phone Management*.
 - Step 2** Select the required *Location* (active text link).
 - Step 3** Select the required *Recording Profile and Recording Option* from the drop-down lists in the relevant *Private Line Settings* section.
 - Step 4** Click the **Modify** button.
-

Note

The recording profiles need to be imported from the respective Unified CM. Available recording options are static and correspond to the version of the Unified CM. The default value for Recording Option is "Call Recording Disabled".

Migration Concerns

For customers with devices / mobility profiles which already have the "agent line" feature enabled, there are some steps required to ensure that Contact Center is deployed correctly. It is necessary to run two OpsTools after the Contact Center server is created and connected to an IPPBX.

For all locations connected to the IPPBX where the new Contact Center server is connected, the following Ops Tools must be run:

- Refresh All Phone Features at a Location
- Refresh All Mobility Features at a Location

Ops Tools can be performed from the main menu at *General Tools > Operations Tools*.

Service Inventory: Billing

When a phone line or mobility line is enabled or disabled for *Call Center Agent Line*, a history table is updated with these changes for the affected fints. This is then used for billing / SI purposes.

Caveats

Where features such as voicemail use a multitenancy flag, the Contact Center feature does not. The feature behaves in a "multitenancy ON" fashion. There is therefore no way to turn multitenancy on or off.

ASCII Fields

The system provides users with the functionality to set alternative ASCII values for specific fields where required (for instance this will be needed for devices that do not support non ASCII characters). The fields include:

- Display (Internal Caller ID)
- Line Text Label
- Alerting Name
- Speed Dial Label

- Busy Lamp Field Label

For these ASCII fields to be available for editing by users, they must first be enabled in the relevant feature display policies and feature groups.

Enabling ASCII fields in the Feature Display Policy

Procedure

To enable the ASCII fields in the feature display policy:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
 - Step 2** Select the relevant *Feature Display Policy* (active text link).
 - Step 3** Enable the following service types:
 - LabelAscii
 - DisplayNameAscii
 - AlertingNameAscii
 - Step 4** Click the **Modify** button.
-

Enabling ASCII fields in the Feature Group

Procedure

To enable the ASCII fields in the feature group:

- Step 1** Browse to *General Administration > Feature Groups*.
 - Step 2** Select the relevant *Feature Group* (active text link).
 - Step 3** Enable the following features:
 - Label Ascii
 - Display Name Ascii
 - Alerting Name Ascii
 - Step 4** Click the **Modify** button.
-

Phone Lines

Procedure

To modify the ASCII fields for phone lines:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select a Phone (active text link).
- Step 3** For each relevant line, enter relevant values for the following fields:
 - Display name ASCII

- Label ASCII
- Alerting Name ASCII

Step 4 Click the **Modify** button.

CTI Route Points

Procedure

To modify the ASCII fields for CTI Route Points:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *CTI Management* (active text link).
- Step 3** Select *CTI Route Points* (active text link).
- Step 4** Select the required *CTI Route Point* (active text link).
- Step 5** For each relevant line, enter relevant values for the following fields:
- Display name ASCII
 - Label ASCII
 - Alerting Name ASCII
- Step 6** Click the **Modify** button.
-

CTI Route Ports

Procedure

To modify the ASCII fields for CTI Route Ports:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *CTI Management* (active text link).
- Step 3** Select *CTI Ports* (active text link).
- Step 4** Select the required *CTI Route Point* (active text link).
- Step 5** For each relevant line, enter relevant values for the following fields:
- Display name ASCII
 - Label ASCII
 - Alerting Name ASCII
- Step 6** Click the **Modify** button.
-

Mobility

Procedure

To modify the ASCII fields for an end user's extension mobility profile, follow these steps

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the required *end user* (active text link).
- Step 3** Click the **Extension Mobility Profile** button.
- Step 4** For each relevant line, enter relevant values for the following fields:
 - Display name ASCII
 - Label ASCII
 - Alerting Name ASCII
- Step 5** Click the **Modify** button.

Busy Lamp Fields

Procedure

To add the ASCII field(s) for a busy lamp field:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select a *phone* (active text link).
- Step 3** Click the **Manage Busy Lamp Fields** button.
- Step 4** Click the **Add** button.
- Step 5** Enter the Label Ascii field.
- Step 6** Click the **Add** button.

Speed dials

Procedure

To add the ASCII field(s) for a speed dial:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select a *phone* (active text link).
- Step 3** Click the **Manage Speed Dials** button.
- Step 4** Click the **Add** button.
- Step 5** Enter the *Label (Ascii)* field.
- Step 6** Click the **Add** button.

Note

- If the *ASCII Label* field is not provided and the standard *Label* field has a valid ASCII value then the standard Label field's value is used for the *ASCII Label* field; but if the standard label is not a valid ASCII value then the

Telephone Number field's value is used for the *ASCII Label* field. (The reverse logic is applied for the normal *Label* field when left blank.)

- For more information on Speed Dials, see [Phone Management on page 803](#).

Bulk loading ASCII values

Bulk loading ASCII values can be done via the *LocAdmin* workbook. The *Ascii Name* field has been added to the *Add User Speed Dials* sheet and to the *Add Phone Speed Dials* sheet.

Importing Device Specific Settings

The system provides a mechanism to import phone specific settings from Cisco Unified Communications Manager (Unified CM), version 8.6.2.21020-1 and newer. For previous versions of Unified CM, this information is imported from static files on the CUCDM. These settings are available in the system admin GUI in the phone management area as advanced settings that can be set, managed, and configured into the Cisco Unified Communications Manager (Unified CM).

As part of this feature, administrators can do the following:

- Import these advanced phone settings from Unified CM and re-import these settings again at a later time; they can do this through the admin GUI or bulk load pages.
- Control which specific advanced phone settings are visible and/or manageable in the admin GUI.
- Control which specific advanced phone settings are visible and/or manageable in the Self Care GUI.
- Manage advanced phone settings on a per phone basis.
- Give access to End Users to manage advanced phone settings.
- Bulk load phones and specify values for the available phone specific settings dynamically.
- Manage/control the values for the advanced phone settings via the web service API.

Run a standalone script to import and apply all advanced phone settings for

- all phone locations of a customer; or
- all phones at a specific location.

This feature will support Unified CM versions 6.1.x and newer.

Importing Advanced Phone Features

Pre-8.6.2.21020-1 Unified CMs

The System administrator can import the advanced phone features from static data files containing the settings for specific versions of Unified CM. This can be done through the admin GUI or a bulk load page.

There is no way to get advanced phone features dynamically from the Unified CM. Static data files were generated with the latest settings for a specific version of a Unified CM. When a new phone type is introduced and loaded into a Unified CM, the high level process for supporting this new phone in the system is:

1. Load the new phone type into system (once support for this phone type has been announced).

2. Get the latest static data files as part of an emergency release (ER). The process of supporting the new phone type ensures that new static files are generated.
3. Import the new settings (using one of the methods below) into CUCDM for the specific Unified CM cluster.

Note

There may be cases where the admin GUI displays advanced phone features for a device that are not yet supported by its associated Unified CM. These unsupported settings are safely ignored by the Unified CM. This scenario could happen with older releases of Unified CM that have not been updated with the latest advanced phone feature or if a Unified CM is updated to a newer version that introduces new settings not supported by the system.

For more information on settings available for import, see the *Advanced Phone Settings Guide*.

Unified CM version 8.6.2.1020-1 and later

When a new phone type is introduced and loaded into a Unified CM, the high level process for supporting this new phone in CUCDM is as follows:

1. Load the new phone type into CUCDM (once this phone type is supported by the system),
2. Import the new settings (using one of the methods below) in CUCDM for the specific Unified CM cluster

Note

There may be cases where the admin GUI displays advanced phone features for a device that are not yet supported by its associated Unified CM. These unsupported settings are safely ignored by the Unified CM. This scenario could happen with older releases of Unified CM that have not been updated with the latest advanced phone feature or if a Unified CM is updated to a newer version that introduces new settings not supported by the system.

Importing Advanced Phone Features via the Admin GUI

Procedure

To import advanced phone features via the GUI:

- | | |
|---------------|---|
| Step 1 | Browse to <i>Network > PBX Devices</i> . |
| Step 2 | Select the required server <i>Name</i> (active text link). |
| Step 3 | Click the Import/Refresh Items button on the <i>CCM Cluster Management</i> screen. |
| Step 4 | Select the checkbox next to <i>Phone Features</i> and click the Import/Refresh Items button. |
-

The phone features are imported from the Unified CM. To view the imported features, browse to the *CCM Cluster Management* Screen, click the **Import/Refresh Items** button, and then click the *Phone Features* active text link.

Importing Advanced Phone Features via Bulk Loading

In the *Network* workbook, the *Import CCM Items* sheet for a given Provider will now have a *Phone Features* column . The *Phone Features* column of a cluster accepts 'Y' or 'N' values. If

Phone Feature is selected ('Y') then the Phone Features will be imported from Unified CM into the system during the bulk load operation.

For more information on bulk loading advanced phone features, please refer to the *Bulk Loader Guide*.

Feature Group setting for Advanced Phone Settings

The admin user can control when the Advanced Phone Features are available to devices by enabling/disabling it in the feature group.

Procedure

To enable the Advanced Phone Features in a feature group:

- Step 1** Browse to *General Administration > Feature Groups*.
 - Step 2** Select the required *Feature Group* (active text link).
 - Step 3** Select the checkbox next to *Advanced Phone Settings* in the *Handset* section.
 - Step 4** Click the **Modify** button.
-

Feature Display Policy Setting for Advanced Phone Settings

Procedure

To enable Advanced Phone Features in a Feature Display Policy:

- Step 1** Browse to *Setup Tools > Feature Display Policies*.
 - Step 2** Select the required Feature Display Policy *name* (active text link).
 - Step 3** In the *Handset* section select the *AdvancedSettings* checkbox to enable the feature.
 - Step 4** Set the *Access Type* by selecting a value from the drop-down list. Setting the Access Type to 'Read Only' will allow read-only access of each individual setting in Self Care, while 'Read Write' will enable the user to modify these settings from Self Care.
 - Step 5** Provide a *Display Name* value to determine what is displayed to the user in Self Care when accessing this feature.
 - Step 6** Click the **Modify** button.
-

Managing Advanced Phone Settings for a Device

Procedure

To manage the Advanced Phone Settings for a specific device:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the *Device Name* (active text link).
- Step 3** In the *Advanced Settings* section, set each individual advanced setting. The settings displayed are dependent on the advanced settings imported from the connected Cisco Unified Communications Manager. Next to each advanced setting, if available, the user can mouse-over a tooltip that provides more information about the setting.

Step 4 Click the **Modify** button.

Managing Advanced Phone Settings in Self Care

End users can manage their advanced phone settings in Self Care on the *Phone Details* screen, accessible via the *My Phones* menu option. End users can view or modify each individual advanced setting, depending on the settings in the relevant *Feature Display Policy*.

Specifying Advanced Phone Settings when Bulk Loading Phones

In the *Modify Phone Features* and *Register Phones* bulk load sheets (in the *LocAdmin* workbook), advanced settings can be added by using the ' *key:value* ' notation.

For more information on bulk loading advanced settings, please refer to the *Bulk Loader Guide*.

Importing Advanced Phone Settings for Existing Devices via CLI

The CLI tool provides easy migration of advanced phone settings from Cisco Unified Communications Manager (Unified CM) to the System. These settings can then be managed by the System. It reads the current advanced settings from Unified CM, and then applies these settings into the new structure supplied by the System. This process prevents the System from overwriting these settings in Unified CM, where they may have been manually configured.

Phone Settings for existing devices can be imported from Unified CM by using the system's command line interface (CLI).

A typical CLI interface call and parameter would be:

```
python import_phone_advanced_settings.py
Please enter the Provider Name: HCS_Provider
Please enter the Reseller Name: Reseller_1
Please enter the Company Name: Customer_1
Perform import for all locations [Y|N]? Y
```

The resultant transaction log for the import can be viewed on the admin GUI by browsing to *General Tools > Transactions*.

See also:

- Command Line Interface (CLI) Guide for more information on the command line interface if required.

Music on Hold Track Management

Adding, viewing, modifying and deleting Music on Hold (MoH) tracks are covered.

Adding a MoH Track

Procedure

Adding a MoH Track

To add a new Music on Hold track:

- Step 1** Browse to *Resources > MoH Tracks*
- Step 2** Click the **Add** button.

Step 3 Complete the required fields.

Step 4 Click the **Submit** button.

The new MoH track will now be added.

Field	Description
MoH Track Name	The name of the track that you would like to add. This is a mandatory field.
Track ID	Note The Track ID selected must match an existing MoH Audio Stream Number on Unified CM. The ID of the track being added. This value is selected from the provided drop-down list.
Description	A description for the track you would like to add. This is an optional field.
MoH Server Name	The name of the server from where you would like to source the track. This value is selected from the provided drop-down list. Note If MoH servers (i.e. the hardware group) are shared between customers, then the tracks on the shared MoH server will be available to all customers. If hardware is specific to one customer, then only that customer's MoH servers and tracks will be available to the customer.

Viewing and Modifying MOH Tracks

Procedure

Viewing and Modifying MoH Tracks

To view and/or modify a Music on Hold track:

Step 1 Browse to *Resources > MoH Tracks*

Step 2 Select the required *MoH track*.

Step 3 View the required fields and if necessary, make the required modifications.

Step 4 Click the **Modify** button.

Procedure

Deleting a MOH Track

To delete a Music on Hold track:

Step 1 Browse to *Resources > MoH Tracks*

Step 2 Select the required *MOH track*.

Step 3 Click the **Delete** button.



CHAPTER 3

Provider Administration

- Adding a Service Provider **672**
- Modifying and Deleting a Service Provider **672**
- International Gateway Usage **673**
- Advanced Telephony Settings **674**
- Delete a Service Provider **675**
- Provider Country Management **675**
 - Adding a country to a Provider **676**
 - View and delete a country withing a Provider **676**
- Feature Group Template Management **677**
 - Add a Feature Group Template **678**
 - Viewing and Modifying Feature Group Templates **678**
- Managing PBX Templates **679**
- IP Addresses and Phones **681**
 - IP Inventory Management **681**
 - Add Phones to the Phone Inventory **684**
- Site Code Management **685**
 - Add a Site Code **685**
- Provider Level Voicemail Service **686**
 - Setting the Provider Preference to use Provider Level Voicemail Service **686**
 - Adding a Provider Level Voicemail Service **686**
 - Add Voicemail Service Pilot Number **687**
 - Voicemail Template Management **687**
 - Voicemail Template Restrictions **688**
 - Associate a Number Range **689**
 - Adding a Location Voicemail Profile **689**
- Adding Administration Users **689**
- Allocating E164 Numbers and Phones to Specific Locations **692**
 - Allocating E164 Numbers to Locations **692**
 - Allocating Phones to a Location **693**

The system enables multiple service providers to manage their telephony service using the same platform. The provider management section enables the creating, modification and deleting of the each of the service providers.

Each service provider owns the network components that support their telephony service. Network components may not be shared between different service providers.

It should also be noted that a single service provider may only operate one hardware set and operate a single dial plan. However, if a specific service provider wanted to operate multiple services using different hardware and dial plans, then multiple service providers could be operated by the same real service provider.

Adding a Service Provider

Procedure

To add a new provider:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required details. Available fields include:

Attribute	Description	Remarks
Name	The name of the Service Provider.	This is a mandatory field, and must be alpha numeric
Description	A description of the Service Provider	-
Address1	Address of the Service Provider.	This is a mandatory field.
Address2	Address of the Service Provider.	This is a mandatory field.
Address3	Address of the Service Provider.	This is a mandatory field.
City	City where the Service Provider is situated.	This is a mandatory field.
State	State where the Service Provider is situated.	-
Country	Country where the Service Provider is situated.	This is a mandatory field. Select from the drop-down list, default = the preferred country of the Admin user doing the Add.
Post/ZIP Code	Post (Zip) code where the Service Provider is situated.	This is a mandatory field.
Contact Name	Contact Name for the person responsible for the provider.	This is a mandatory field.
Contact Telephone Number	Contact telephone number for the person responsible for the provider.	This is a mandatory field.

- Step 4** Click the **Add** button. The new Provider is created within the system.

Modifying and Deleting a Service Provider

Procedure

To modify a provider:

- Step 1** Browse to *Provider Administration > Providers*.
 - Step 2** Select the *provider* (active text link) that you would like to modify.
 - Step 3** Make the required changes then click the **Modify** button to save your changes. The changes made to the provider are saved to the system.
-

Procedure

Delete a Service Provider

Follow these steps to delete a Provider:

- Step 1** Browse to Provider Administration > Providers
 - Step 2** Select the Provider (active text link) that you would like to delete.
 - Step 3** Select the **Delete** button.
 - Step 4** After confirming the delete operation, the Provider is deleted.
-

Important

You cannot delete a Provider while there are Customers allocated to that Provider. The customers must be deleted before a Provider can be deleted.

International Gateway Usage

This page enables providers to manage the countries in the international gateways. In the CUCDM, international gateways relates to transit switches. PGW and SME are currently the only supported transit switches in the CUCDM.

Procedure

To add a country to an international gateway:

- Step 1** Browse to *Provider Administration > Providers* .
 - Step 2** Select the *Provider* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt** button.
 - Step 4** Click the **International Gateway Usage** button.
 - Step 5** Select the relevant *Transit Switch* (active text link).
 - Step 6** Click the **Add** button.
 - Step 7** Provide all of the required fields.
 - Step 8** Click the **Add** button. The country is added to the Gateway.
-

Procedure

To delete a country from an international gateway:

- Step 1** Browse to *Provider Administration > Providers* .
- Step 2** Select the *Provider* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **International Gateway Usage** button.
- Step 5** Select the relevant *Transit Switch* (active text link).
- Step 6** Select the *Delete* (active text link) adjacent to the country that you would like to remove.

After confirming the deletion, the country is removed from the gateway.

Note

Depending on the configuration of your system, confirmation may not be requested when deleting a country.

Advanced Telephony Settings

This page enables providers to manage their advanced telephony settings. Currently, the available settings include:

- `FwdRedirectingExternalNumonCallFwd`

FwdRedirectingExternalNumonCallFwd

The `FwdRedirectingExternalNumonCallFwd` setting is used to manage the *AssociateFNN-Redirect* and *DisassociateFNN-Redirect* transactions. This setting drives the use of the AssociateFNN-Redirect model. The purpose of the feature and model is to include a mapping in the TimesTen DB for calls being forwarded to the PSTN. In the case where the calling number matches an entry, its FNN would be used as the CLI for the call (instead of the default behavior of site published number). Basically, the transaction takes all FNNs associated with a fint number and applies the redirect script(s) to the TimesTen driver.

- The default for this setting is *Off* (Disabled)
- This setting has the potential to modify all FNNs for the provider
- Depending on the size of the provider, this may take a long time to execute
- This setting may be overridden at the Customer and Location Level

Procedure

To activate the AssociateFNN-Redirect transactions:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the *Provider* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Advanced Telephony Settings** button.
- Step 5** Select the checkbox adjacent to `FwdRedirectingExternalNumonCallFwd`.

- Step 6** Click the **Apply** button. After confirming the operation, the *AssociateFNN-Redirect* transactions are activated.

Procedure

To deactivate the DisassociateFNN-Redirect transactions:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the *Provider* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt** button.
- Step 4** Click the **Advanced Telephony Settings** button.
- Step 5** De-select the checkbox adjacent to *FwdRedirectingExternalNumonCallFwd*.
- Step 6** Click the **Apply** button.

After confirming the operation, the *DisassociateFNN-Redirect* transactions are deactivated.

Delete a Service Provider

Procedure

To delete a provider:

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the *Provider* (active text link) that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the provider is deleted from the system.

Note

You cannot delete a provider while there are customers allocated to the provider. The customers must be deleted before a provider can be deleted.

Provider Country Management

The system enables providers to operate in a multi-country environment. Each country however, has unique dial plan elements and number configurations, so the system has to apply these different configurations to each location based on the country in which they are allocated. Hence, countries can be managed from two sections within the system, the *Dial Plan* menu and from the *Provider Administration* menu.

Procedure

OffNet Status

To view the configured prefixes for a country:

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Select the *Country* name (active text link) of the country that you would like to view.

Step 3 Click the **Force OffNet** button.

A list of all configured prefixes is displayed. The standard Quick Search functionality is available for searching the list.

Procedure

Adding a Prefix to a country

To add a prefix to a country:

Step 1 Select the *Provider Countries* tab in the *Provider Administration* menu.

Step 2 Select the *Country* name (active text link) of the country that you would like to modify.

Step 3 Click the **Force OffNet** button.

Step 4 Enter a Prefix and click the **Add** button.

The Country is updated within the system.

Procedure

Deleting a Prefix from a country

To delete a prefix from a country:

Step 1 Select the *Provider Countries* tab in the *Provider Administration* menu.

Step 2 Select the *Country* name (active text link) of the country that you would like to modify.

Step 3 Click the **Force OffNet** button.

Step 4 Click the **Delete** button adjacent to the prefix that you would like to delete.

The Country is updated within the system.

Adding a country to a Provider

Procedure

Add a Country to a Provider

Step 1 Select the *Provider Countries* tab in the *Provider Administration* menu.

Step 2 Click the **Add** button.

Step 3 Select the relevant Country from the drop-down list and click the **Add** button.

The Country is added to the provider within the system.

View and delete a country withing a Provider

Procedure

View Countries Within a Provider

To view a country:

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Select the *Country* name (active text link) of the country that you would like to view.

The system displays the relevant details of the selected country.

The following fields are available when viewing a country at the provider level:

Field	Description
Country	The name of the country being viewed. For example, "United Kingdom".
ISO Country Code	The ISO code for the country being viewed, the system completes this field for you when adding a country. For example, for the United Kingdom, the ISO code displayed is "GBR".

Procedure***Delete a Country***

To delete a country from a provider:

- Step 1** Select the *Provider Countries* tab in the *Provider Administration* menu.
- Step 2** Select the *Country* name (active text link) of the country that you would like to delete.
- Step 3** Click the **Delete** button.
- Step 4** After confirming the deletion operation, the country is deleted from the system.

Feature Group Template Management

All telephony and value added features managed by the system are defined as Features. Any single version of the system supports a defined set of features. These features are then Grouped together to form a Feature Group, which is then associated with a phone or user and defines the set of features the person or phones has access to. Feature groups are the primary means for managing the Class of Service for users. The system enables administrators to specify Feature Group Templates. These templates enable administrators to quickly and effectively roll-out common feature groups such as office phones and boardroom.

Note

Feature Groups are traditionally customized on the Customer level, by the Customer.

The Feature Group Template Management screen enables you to view, add, delete and modify feature group templates.

Procedure***Viewing available Feature Group Templates***

To view available Feature Group Templates:

- Step 1** Browse to *Provider Administration > Feature Group Templates*. A list of the available Feature Group Templates is displayed.
- Step 2** To see further details for a specific Feature Group Template, select the *Name* (active text link) of the required Feature Group Template. The feature group template details are displayed.
-

Add a Feature Group Template

Procedure

Add a Feature Group Template

To add a Feature Group Template:

- Step 1** Browse to *Provider Administration > Feature Group Templates*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields. For a list of fields available refer to [Features Available when Adding or Modifying a Feature Group on page 505](#).

Note

The list of available fields may differ based on the configuration of your system.

- Step 4** Click the **Add** button. The feature group template is added to the system.
-

Viewing and Modifying Feature Group Templates

Feature groups are the primary means for managing the Class of Service for users. The system enables administrators to specify Feature Group Templates. These templates enable administrators to quickly and effectively roll-out common feature groups such as office phones and boardroom.

Note

Feature Groups are traditionally customized on the Customer level, by the Customer.

Procedure

Viewing available Feature Group Templates

To view available Feature Group Templates:

- Step 1** Browse to *Provider Administration > Feature Group Templates*.
- A list of the available Feature Group Templates is displayed.
- Step 2** To see further details for a specific Feature Group Template, select the *Name* (active text link) of the required Feature Group Template.
-

The feature group template details is displayed.

Procedure

Modify a Feature Group Template

To modify a Feature Group Template:

- Step 1** Browse to *Provider Administration > Feature Group Templates*.
- Step 2** Select the *Name* (active text link) of the Feature Group Template that you would like to modify.
- Step 3** Make the required modifications to the relevant fields.

The following fields are available when modifying a Feature Group Template. For a list of fields available refer to [Features Available when Adding or Modifying a Feature Group on page 505](#):

Note

The list of available fields may differ based on the configuration of your system.

- Step 4** Click the **Modify** button when complete.

The feature group template is updated in the system.

Procedure

Delete a Feature Group Template

To delete a Feature Group Template:

- Step 1** Browse to *Provider Administration > Feature Group Templates*.
- Step 2** Select the *Name* (active text link) of the Feature Group Template that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion operation, the feature group template is deleted from the system.
-

Managing PBX Templates

All PBX features and functionality managed by the system are defined as PBX Features. Any single version of the system supports a defined set of PBX features. These features can be grouped into PBX templates, a PBX template being a pre-configured set of PBX features. PBX templates are used mainly when adding a new Location and are the primary means for managing available PBX services and features. The system enables administrators to specify PBX templates. These templates enable providers to quickly and effectively roll-out common PBX configurations.

Note

- If no PBX templates are configured when adding a new location, the default PBX template is used.
 - You can search for PBX templates using a PBX template name, simply enter your search term in the search field and click the **Search** button. A list of all matching template names is returned.
-

The PBX template Management screen enables you to view, modify, add, and delete PBX templates.

Procedure

Viewing Available PBX Templates

To view available PBX templates:

- Step 1** Browse to *Provider Administration > PBX Templates*. A list of the available PBX templates is displayed.
- Step 2** To see further details for a specific PBX template, select the Name (active text link) of the required PBX template.
-

The PBX template details are displayed.

Procedure

Adding a PBX Template

To add a PBX template:

- Step 1** Browse to *Provider Administration > PBX Templates*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields. The following fields are available when adding a PBX template:

Field	Description	Remarks
Name	The name of the PBX template being added.	This is a mandatory field.
Description	A short description of the PBX template being added.	-

- Step 4** Click the **Add** button. The PBX template is added to the system.
-

Procedure

Modify a PBX Template

To modify a PBX template:

- Step 1** Browse to *Provider Administration > PBX Templates*.
- Step 2** Select the *Name* (active text link) of the PBX template that you would like to modify.
- Step 3** Make the required modifications and click the **Modify** button. The PBX template is updated in the system.
-

Procedure

Delete a PBX Template

To delete a PBX template:

- Step 1** Browse to *Provider Administration > PBX Templates*.

- Step 2** Select the *Name* (active text link) of the PBX template that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the PBX template is deleted from the system.
-

IP Addresses and Phones

IP Inventory Management

The IP Subnet Management screen lists all of the existing managed IP subnets. This list also provides information as to which Customer and Location the managed IP subnet is allocated to.

For ease of use, the system provides users with an managed IP subnet search function. For help on using quick search, please see [Quick Search on page 534](#).

Note: Since the default number of managed IP subnets listed on this page is 50, you may need to use the Search function to find the relevant managed IP subnet. To do this, change the default result number to greater than 50 and select the **Search** button.

Note: If you do not fully understand IP addressing, we recommend that you read some additional background information before proceeding.

An IP subnet is a logical group of IP Addresses, normally based on the private address range within a Provider or Customer. A unique IP address range (or subnet) is assigned to each Location. The system manages the IP subnets for each location, these subnets can be of various sizes, depending on the size of the Location. The system enables a Location to have multiple subnets and you can also share a single subnet between two different locations.

Each phone within the system must have a unique IP address. The system will not allow an operator to allocate incorrect IP subnet addresses to a location.

The system supports both PAT and NAT based subnets:

- NAT (Network Address Translation) is standard that enables a local area network (LAN) to use one set of IP addresses for internal network traffic and a second set of addresses for external traffic.
- PAT (Port Address Translation) is a form of network address translation whereby each IP Address on the LAN is translated to the same IP address but each with a different port.

Note

- The system only supports PAT with a 32 bit subnet.
 - By default, subnets are added as NAT.
-

Adding an IP Subnet

Procedure

If you are a Provider Administrator, you must create IP subnets when setting up a new platform and when the platform grows beyond the initial quantity of subnets.

IP subnets can be added in two manners, the most popular is via a batch job by adding bulk subnet groups then allocating these subnet groups to Customers case by case. Alternatively, you can add

subnets manually via the IP Inventory Management page. For information on adding subnets manually, please see Adding an IP Subnet below. The system recommends using the bulk loader method, as it is generally faster to use the IP inventory Bulk Loader to create IP subnets when setting up new customers and locations.

To add an IP subnet:

- Step 1** Browse to *Resources > Managed IP Subnets*.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields. The following table describes the fields available on the *Add IP Subnet* screen.

Field	Description
<i>IP Subnet</i>	The required subnet should be entered as a standard IP subnet format. For example 10.0.1.0. This is a mandatory field.
<i>Subnet Mask</i>	The number of bits masking the Network portion of the IP Addresses in the subnet. This is a mandatory field.
<i>Shareable across locations?</i>	Select this checkbox if you would like the subnet to be accessible from multiple locations.
<i>DHCP Server Controlling this Subnet</i>	The IP address of the DHCP server that manages this IP Subnet. Select the required server from the drop-down list. For managed subnets, this tells the system which DHCP server to provision for the subnet. For unmanaged subnets, this setting is still required but any available DHCP server can be selected. This is a mandatory field.
<i>IP Edge Device</i>	The name of the routing device on this subnet. Select the required IP edge device from the drop down list. This is used to create the mapping of the subnet to the IP Edge device. This is a logic mapping to the device.
<i>Origin IP of DHCP messages encapsulated by router</i>	The IP address that is displayed as the source of messages encapsulated by the router. This setting, and the setting below, relate to the DHCP-based AutoMove capability in the system. These settings allow the system to map the source addresses of the DHCP requests to this subnet to identify the location to move to and subnet to allocate the address from. The alternate setting is in case the DHCP requests are not all from the same source address. One example is that in a network with IOS devices setup with HSRP as the default route, the DHCP requests are sourced with the physical interface of the IOS devices (typical the vlan interface address) instead of the virtual HSRP address. In this instance, both the Origin and Alternate Origin need to be configured: one with the IP address for device 1 and one with the IP address for device 2. The system's DHCP logs or DHCP packets on the network can be inspected to determine the source addresses if AutoMove is not working as expected. This is a mandatory field.
<i>Alternate Origin IP of DHCP messages (HSRP paired routers)</i>	A secondary IP address that is displayed as the source of messages encapsulated by the router. For more information, please see the field above.
<i>DHCP helper IP address</i>	The IP address of the main DHCP server to which the IP Edge device sends the request. This is a mandatory field.
<i>Backup DHCP helper IP address</i>	The IP address of the backup DHCP server to which the IP Edge device sends the request.
<i>Domain Name</i>	The DNS domain name used by the phones.

Field	Description
<i>Primary DNS server IP</i>	The IP address of the primary DNS server to which phones send their DNS queries. This is a mandatory field.
<i>Fallback DNS server IP</i>	The IP address of the secondary DNS server to which phones send their DNS queries. This is a mandatory field.
<i>IP address for default route of Phone</i>	The IP address of the default routing device on the phone network. This is relevant to system managed subnets where the DHCP configuration requires the default gateway setting as part of the subnet definition. This is a mandatory field.

Step 4 Click the **Add** button when complete. The managed IP subnet is added to the system.

Note

The range of IP addresses in the added IP subnet is validated against current usage in CUCDM. IP addresses used by *Origin IP of DHCP messages encapsulated by router*, *Alternate Origin IP of DHCP messages (HSRP paired routers)*, and *IP address for default route of Phone* (see fields above), as well as those excluded by the bulk load process are automatically made inactive.

Modifying a Managed IP Subnet

Procedure

To modify the details in a managed IP subnet:

- Step 1** Browse to *Resources > Managed IP Subnets*.
- Step 2** Select the *IP Subnet* (active text link) of the managed IP subnet that you would like to modify.
- Step 3** Make the relevant changes to the managed IP subnet, and then click the **Modify** button. The managed IP subnet is updated with the modifications. Refer to [Adding an IP Subnet on page 681](#) for field descriptions.

Note

Modified IP addresses are validated against current usage in CUCDM. IP addresses used by *Origin IP of DHCP messages encapsulated by router*, *Alternate Origin IP of DHCP messages (HSRP paired routers)*, and *IP address for default route of Phone* (see fields above), as well as those excluded by the bulk load process are automatically made inactive.

Procedure

Deleting a Managed IP Subnet

There are two methods for deleting managed IP subnets. Using the first method to delete a managed IP Subnet:

- Step 1** Browse to *Resources > Managed IP Subnets*.
- Step 2** Select the *Delete* link adjacent to the managed IP subnet that you would like to delete. After confirming the deletion, the managed IP subnet is deleted from the system.

Alternatively, delete a managed IP subnet as follows:

- Step 3** Browse to *Resources > Managed IP Subnets*.

Step 4 Select the *IP Subnet* (active text link) of the managed IP Subnet that you would like to delete.

Step 5 Click the **Delete** button at the bottom-right of the screen. After confirming the deletion, the managed IP subnet is deleted from the system.

Note: You must remove the managed IP Subnet from its Location before you can delete it. To do this you go to the *Manage Location* screen and select the **Manage IP Subnet** button.

Single IP Address Management

An IP Subnet is a logical group of IP Addresses, normally based on the private address range within a Provider or Customer. A unique IP address range (or Subnet) is assigned to each Location. The system manages the IP Subnets for each location, these subnets can be of various sizes, depending on the size of the Location. The system enables a Location to have multiple subnets and you can also share a single subnet between two different locations.

Procedure

Managing Single IP Addresses

The system enables you to manage IP addresses individually.

To manage a single IP address:

Step 1 Browse to *Resources > Managed IP Subnets*.

Step 2 Select the *IP Subnet* (active text link) of the IP Subnet that contains the IP address that you would like to manage.

Step 3 Click the **Manage Individual IP Addresses** button.

Step 4 To make an IP address active, select the *Make Active* text link adjacent to the IP address.

or

To make an IP address inactive, select the *Make Inactive* text link adjacent to the IP address.

Step 5 To exit, select the *Return to IP Subnets* link.

The IP Addresses is now active and/or inactive within the system.

Viewing the Associated Device

If a device (phone) is allocated to an IP address, the device name of the related device is displayed as an active text link adjacent to the relevant IP address. Selecting this active text link display the *Phone Inventory* information page.

Add Phones to the Phone Inventory

Adding a phone can be performed at the Reseller, Customer, Division or Location administration level, depending on the configuration of the relevant administrator's access profile settings.

Regardless of the point in the hierarchy you are when adding a phone, it is added at the Service Provider level unless it has been assigned to a specific hierarchy level.

Procedure

To add a phone:

- Step 1** Browse to *Resources > Phone Inventory*.
- Step 2** Click the **Add Phone** button.
- Step 3** Complete the required fields. The following fields are available when adding a phone:

Field	Description	Notes
Phone Type	New phone type	Default is the 1st value in list.
Enter the MAC address of the phone	Specify the MAC address (device name) of the device.	The MAC address (device name) is validated according to the device name format for the device's phone type.
Full device name	The full device name the system used to manage the device.	This field is populated by the system.
Configuration Profile	This setting is used to mark the phone as a dummy phone to be replaced later as part of phone based registration of an actual phone. See Phone Based Registration on page 788 for more information.	Enable only if this is not a real device.

- Step 4** Click the **Add Phone** button.

Site Code Management

Each Customer Location managed by the system has a Site Code. This is either automatically allocated or selected by an administrator. In order for the system to allocate or enable Site Codes to be selected, they must have been defined in the system. The Site Code Management screens enable the definition and deletion of these Site Codes.

Sites Codes are a numeric string, the format of which is defined by the specific of the associated Dial Plan. Site Code should therefore only be entered/defined by suitably qualified personnel who have an appropriate knowledge of the Dial Plan.

Site Codes are used in environments where a Customer has more than one Location. This code is then used by end users calling from one Location to another as follows:-

Site X is Site Code 2555

Site Y is Site Code 4567

In order for a user in Site X to call extension 7890 in Site Y, they must dial 45677980.

Add a Site Code

To add a site code, browse to *Resources > Site Code Inventory* and follow the steps as described in [Site Code Management for Buildings on page 727](#).

The following fields are available when adding a site code:

Field	Description
Site Code Rules	The rules that apply for new site codes, for example, "Site Code Max 4 digits".
Site Code	The site code being added. This must comply with any rules defined in the above field. This is a mandatory field.

Field	Description
Last Site Code in range	This is an optional field and is used to define the last site code in a range of site codes.

For more information on site codes for dial plans and for an explanation of the site code fields, see:

- [Dial Plan Management on page 54](#)

Provider Level Voicemail Service

This section details how a voicemail service can be defined and used at the provider level.

Setting the Provider Preference to use Provider Level Voicemail Service

To use the provider level voicemail service, the provider level preference *MultitenantVoiceMail* needs to be set as false.

Procedure

To configure the setting:

- Step 1** Browse to *Provider Administration > Provider*.
- Step 2** Select the *Provider* for which the setting needs to be configured.
- Step 3** Click the **Preferences** button.
- Step 4** Select the MultitenantVoicemail link and set it to false.

Note

If this setting is true, the Voicemail Services is available at the Customer Level.

Adding a Provider Level Voicemail Service

Connect Voicemail Server to PBX/ Transit

A voicemail service needs to be associated to a voicemail server when it's added. The associated Voicemail server should be connected to PBX or Transit servers so that the add voicemail service configuration can be applied to them.

Procedure

To connect a Voicemail Server to a PBX/Transit:

- Step 1** Browse to *Network > Voicemail Servers*.
- Step 2** Click the **VM Server=> Transit** button to connect a transit to a Voice Server or **VM Server=>PBX** to connect a PBX to a Voicemail Server. This leads to a screen that allows connecting/disconnecting these components to the voicemail server.

Alternatively:

The voicemail server can also be connected to a PBX by browsing to *Network > PBX devices*, selecting the **Connectivity** button, and then clicking the **PBX=>Voicemail** button.

The voicemail server can also be connected to a transit by browsing to *Network > Transit Switches*, and then clicking the **Transit=>VMServer** button.

Add Voicemail Service

To add a voicemail Service at the provider level, browse to *Resources > Voicemail Services* and click the **Add** button. Under details, the following mandatory settings need to be configured:

- **Name**
- **Country**: Select from the list of countries provided in the drop-down.
- **Site Code**: It should be a number and less than the maximum length of site code allowed.
- **Voice Mail Server**: Select from the list provided.
- **Extension Length**: Length of extension for finnumber inventory, which would be added for the voicemail Service. Select from the list provided.
- **Voicemail PSTN Dial Prefix**: Select from the list provided.

The Voicemail service configuration is applied to the Transits and PBXs which are connected to the Voicemail Server.

Add Voicemail Service Pilot Number

To add a voicemail service pilot number, browse to *Resources > Voicemail Services* and select the **Voicemail service** for which the pilot number needs to be added, click the **Pilot Number** button and then click the **Add** button.

Under details, the following mandatory settings need to be configured:

- **Pilot Number**: Select from the list of extension numbers available from voicemail service internal number inventory
- **Domain Name**:
- **Call Agent**: Select from the provided list of PBXs and Transits connected to the Voicemail server associated to the voicemail service.

Voicemail Template Management

Voicemail template management allows you to view which voicemail service types have been enabled. This page also allows you to access the page in order to impose restrictions on the functionality of voicemail services available to end-users that are subscribed to the Voicemail service by clicking the **Restrictions** button.

Procedure

View and Modify a Voicemail Template

To view and modify a Voicemail template:

- Step 1** Select the *Voicemail Services* tab in the *Resources* menu.
- Step 2** Select the Voicemail Service *Name* (active text link) of the Voicemail Service that you would like to view.
- Step 3** Click the **Voicemail Template Mgt** button.
- Step 4** View the available voicemail types, as well as the current status of each type, i.e. checkbox enabled (selected) or not.

- Step 5** Modify the status of the voicemail service type if required by selecting or clearing the appropriate *Select* checkbox, and then clicking the associated **Update** button.
- Step 6** Click the relevant **Restrictions** button if you wish to impose restrictions on the functionality of voicemail services available to end-users that are subscribed to the Voicemail service.

Voicemail Template Restrictions

Provider, reseller or customer administrators can impose restrictions on the functionality of voicemail services available to end-users who are subscribed to the Voicemail service.

Procedure

To set restrictions for Voicemail templates:

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Select the required Voicemail Service *Name* (active text link). The *Manage Voicemail Services* screen is displayed.
- Step 3** Click the **Voicemail Template Mgt** button. The *Voicemail Template Management* screen is displayed.
- Step 4** Click the **Restrictions** button adjacent to the relevant Voicemail service type on which you want to impose restrictions. The *Voicemail Template Restrictions* screen is displayed.
- Step 5** Set the required restrictions. The following fields are available when setting Voicemail Template restrictions:

Field	Description	Remarks
Notification Devices		
SMS	Set the number of SMS notifications that are available to subscribers of the selected voicemail service.	0 - 9
Phone	Set the number of phone notifications that are available to subscribers of the selected voicemail service.	0 - 9
Email (SMTP)	Set the number of email notifications that are available to subscribers of the selected voicemail service.	0 - 9
Pager	Set the number of pager notifications that are available to subscribers of the selected voicemail service.	0 - 9
Alternate Extensions		
Alt Ext	Set the number of alternate extension numbers that are available to subscribers of the selected voicemail service.	0 - 9
Caller Input		
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #	Select the checkboxes adjacent to each available caller input. The selected caller inputs are made visible to end users in Self Care so that end users can configure the respective caller inputs themselves.	0 - #

- Step 6** Click the **Modify** button to implement the restrictions on the selected Voicemail service type.

Note

Click the **Reset Counters** button (if required) to reset all counters for both *Notification Devices* and *Alternate Extensions* to 0.

Associate a Number Range

Procedure

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Select a Voicemail Service *Name* (active text link).
- Step 3** Click the **PSTN Number Mgt** button followed by the **Associate Range** button.
- Step 4** Select from the drop-down list the country and national codes of the FNNs available to the Voicemail Service.

For more information on how to make number ranges available to the Voicemail Service, see [Move Number Range on page 578](#).
- Step 5** Select the number range to complete the association.

Adding a Location Voicemail Profile

A voicemail service needs to be added to the location level so that it can be used in that location. To add a voicemail service at the location level:

Procedure

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the Location *Name* (active text link) to which the voicemail profile needs to be added.
- Step 3** Click the **Advanced Mgt.** button and then the **Voicemail Management** button.
- Step 4** Click the **Voicemail Profile Mgt** button.
- Step 5** Click the **Add** button.

Under *Details* the following settings should be configured:
 - *Voicemail Name*
 - *Voicemail Profile Name*: Enter a unique name (up to 50 alphanumeric characters - no spaces). This is a mandatory field.
 - *Description*: Enter a brief description (up to 50 characters).
 - *Pilot Number*
 - *Box Mask*: Enter the box mask (up to 50 characters).
- Step 6** Click the **Submit** button when complete.

This adds a voicemail profile and pilot number to the PBX supporting the location to which the voicemail service is being added.

Adding Administration Users

Administration users are added to the system to perform the different tasks necessary to make the system operational.

When you create an administration user from the *General Administration* menu, a user account with an admin user role is added to the system's database and linked to the administration level specified by the administrator who is currently logged in and adding the new admin user. (Administrators can only add a new administrator or modify the details of an existing administrator at a level lower than their own level in the administration hierarchy.)

Procedure

To add a new administration user:

Step 1 Browse to *General Administration > Administration Users*.

Note

Admin Users cannot be added via the *Location Administration > End User* menu option.

Step 2 Click the **Add** button at the top of the user list.

Step 3 Enter the end user's details. The fields available in this section of the screen are to do with basic user information. The following fields are available:

Field	Description	Remarks
Username	The id of the user	This is a mandatory field. Must be unique across the platform. Note Best Practice: Consider user name convention see above.
Password	Initial password for user login into the system	This is a mandatory field.
Role	User role in the platform	Select the relevant administration level for the new admin user from the drop-down list.
Title	Title of user	-
First Name	First Name of user	-
Middle Name	Middle name of user	-
Last Name	Last Name (Surname) of user	This is a mandatory field.

Note

Required fields are indicated by a red asterisk (*).

Additional user details for information purposes only:

Field	Description	Remarks
Home Telephone Number	Home telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Mobile Telephone Number	Mobile telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Contact Telephone Number	Contact telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.

Field	Description	Remarks
Alternative Telephone Number	Alternative telephone number for user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Email Address	User email address	Note Best Practice: Although not a mandatory field, it is useful to set up users with their correct email addresses.
Job Title	Job title of user	-
Directory Filter	-	-
Information	Additional Information for user	-
Misc	-	-
Welcome Message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-

Step 4 After completing the relevant fields on this page, click the **Next** button.

Note

Required fields are indicated by a red asterisk (*).

Step 5 Complete the required fields (see table below)

Field	Description	Remarks
GUI Branding	The branding theme (colors, fonts, items look & feel etc.) to be presented to the user when they log in to the system.	Select from the drop-down list. The branding themes are defined by the Provider administrator. The applicable branding themes should be enabled for each level in the system hierarchy.
Preferred Country	The country to which the admin user is linked.	Select from from the drop-down list.
Access Profile	Defines the system's menu options available for the user.	Select from the drop-down list. Default access profile is provided as part of the product. The available access profiles are defined by the Provider Administrator. Note The values in the drop-down list are the values that were entered in the <i>Description</i> field when the Access Profiles were added to the system.

Field	Description	Remarks
Override Language	Select from the drop-down list a language to apply as the admin user's default language.	<p>The 'default' option keeps the default language of the hierarchy entity to which the user belongs, i.e. location default language for location administrators, customer default language for division and customer administrators.</p> <p>Note</p> <p>This field is only available if the <i>Enable Admin GUI Translation</i> field has been set for the associated Customer.</p>
Security Profile	Select the required security profile from the drop-down list.	
Account number to use in external accounting system	If you are using an external accounting system, enter the account number here.	

Step 6 Click the **Add** button. The user account is added to the database.

Allocating E164 Numbers and Phones to Specific Locations

Once you have added your E164 numbers and phones to the inventory, you need to allocate them to the locations where they will be used.

Note

You do not need to allocate IP subnets to locations as the system does this automatically.

Allocating E164 Numbers to Locations

Procedure

To allocate a range of E164 numbers to a location:

- Step 1** Browse to *Resources > E164 Inventory*.
- Step 2** Select the country to which you want to add the number range then click the **Next** button.
- Step 3** Select a national area code from the drop-down list then click the **Next** button.
- Step 4** Click the **Move Number Range** button.
- Step 5** Complete the required fields. The following fields are available:

Field	Description	Remarks
Select Location	Target location to move numbers to	Default is the first location in the list
Start of Number Range	First number in the range you wish to move	The numbers available in the drop-down list are only the ones which are not yet allocated to any location

Field	Description	Remarks
End of Number Range	Last number in the range you wish to move	The numbers available in the drop-down list are only the ones which are not yet allocated to any location

- Step 6** Click the **Move** button. The range of numbers is allocated to the specified location.
-

Allocating Phones to a Location

Procedure

To allocate a phone to a location:

- Step 1** Browse to *Resources > Phone Inventory*.
- Step 2** Select the Device *Name* of the phone that you would like to move.
- Step 3** Click the **Next** button.
- Step 4** Select a move target (desired location) from the drop-down list then click the **Next** button.
- Step 5** Select an IP subnet (not applicable for unmanaged subnets) from the drop-down list, and then click the **Move Phone** button. The phone is allocated to the specified location.
-



CHAPTER 4

Reseller Administration

Resellers	694
Adding a Reseller	694
Managing a Reseller	695
Managing Reseller Administrators	696
Adding an Administrator	696
Modifying an Administrator	699
Reset an Administrator's Password	699
Deleting an Administrator	699

Resellers

Resellers are the entities to which customers are directly related. A service provider may have one or more dedicated resellers who are able to sell and manage the telephony service provided by the service provider. The *Reseller Management* section enables administrators to create, modify and delete resellers.

- It should be noted that the reseller does not own the physical network components supporting the service, but may simply resell the service provided by the service provider.
- When adding large numbers of resellers, it is more efficient to use bulk loading to add the Resellers. Please see the *Bulk Loader* guide for more information.
- The features available at the Reseller level can only be accessed by administrators at the reseller level or higher. These administrators are usually added to the system when the Resellers are added.

Adding a Reseller

Procedure

Adding a Reseller

To add a reseller:

- Step 1** Browse to *General Administration > Resellers*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields. The following fields are available:

Field	Description	Remarks
Name	The name of the reseller.	Must be alpha numeric and is a mandatory field.
Description	A description of the reseller.	-

Field	Description	Remarks
Address 1	Enter the address of the reseller.	-
Address 2	Enter the address of the reseller.	-
Address 3	Enter the address of the reseller.	-
City	Enter the city of the reseller.	-
State	Enter the state of the reseller.	-
Country	The country of the reseller.	This is a Mandatory Field. Select the relevant country from the drop-down list, default = the country of the provider to which the reseller is being added.
Post/ZIP Code	The Post/zip code of the reseller.	Enter the Post/zip code of the reseller.
Contact Name	The contact name for the reseller	Enter the contact name for the reseller.
Telephone Number	The telephone number for the reseller.	Enter the telephone number for the reseller.
Contact Email	The contact email for the reseller.	Enter the contact email for the reseller.
Account number to use in an external accounting system.	If an external accounting system is being used, specify the account number to use.	
Security Profile	The selected security profile.	Select the required security profile from the drop-down list.
Line Types		
This section enables the type and quantity of each line type to be available to the Reseller to be defined. It should be noted that lines can only be offered to customer Locations if sufficient lines are available to the reseller. These are mandatory fields.		
Phone Types		
This section enables the type and quantity of each Phone type to be available to the Reseller to be defined. It should be noted that phones can only be offered to customer Locations if sufficient phones are available to the reseller. These are mandatory fields.		
Service Types		
This section enables the type and quantity of each service type to be available to the reseller to be defined. It should be noted that services can only be offered to customer locations if sufficient services are available to the reseller.		
GUI Branding		
Default Branding of User Interface	Defines the default branding to be used. These are mandatory fields.	
Please select required Branding	Select the branding that are to be available to this service provider	

Step 4 Click the **Add** button. The reseller is added to the system.

Managing a Reseller

Procedure

Modifying a Reseller

To modify a reseller:

- Step 1** Browse to *General Administration > Resellers*.
 - Step 2** Select the Reseller *Name* (active text link) that you would like to modify.
 - Step 3** Make the required changes to the reseller (see [Adding a Reseller on page 694](#) if required for available fields), and click the **Modify** button. The reseller is updated in the system.
-

Procedure

Managing a Reseller's Preferences

Global Settings are a collection of high level system tools that enable administrators to perform system wide changes to the system.

To use one of the tools:

- Step 1** Navigate to *Global Settings > Setup Tools*.
 - Step 2** Select the System *Tool* (active text link) that you would like to run.
 - Step 3** Specify the required variable and/or options then click the **Modify** button.
-

The system tool runs and the relevant changes are made to the system.

The list of available tools depends on the configuration of your system.

Procedure

Deleting a Reseller

To delete a reseller:

- Step 1** Browse to *General Administration > Resellers*.
 - Step 2** Select the Reseller *Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button. The reseller is deleted from the system.
-

Managing Reseller Administrators

Adding, modifying and managing of reseller administrators is covered in this section.

Adding an Administrator

Admin users are added to the system to perform the different tasks necessary to make the system operational.

When you create an administration user from the *General Administration* menu, a user account with an admin user role is added to the system's database and linked to the administration

level specified by the administrator who is currently logged in and adding the new admin user. (Administrators can only add a new administrator or modify the details of an existing administrator at a level lower than their own level in the administration hierarchy.)

Procedure

To add a new administration user:

Step 1 Browse to *General Administration > Administration Users*.

Note

Admin Users cannot be added via the *Location Administration > End User* menu option.

Step 2 Click the **Add** button at the top of the user list.

Step 3 Enter the end user's details. The fields available in this section of the screen are to do with basic user information. The following fields are available:

Field	Description	Remarks
Username	The id of the user.	This is a mandatory field. Must be unique across the platform. Best Practice: Consider user name convention see above
Password	Initial password for user login into the system.	This is a mandatory field.
Role	User role in the platform.	This is a mandatory field. Select the relevant administration level for the new administration user from the drop-down list.
Title	Title of user.	-
First Name	First Name of user.	This is a mandatory field.
Middle Name	Middle name of user.	-
Last Name	Last Name (Surname) of user.	Sometimes referred to as Surname. This is a mandatory field.

Note

Required fields are indicated by a red asterisk (*).

Additional user details for information purposes only:

Field	Description	Remarks
Home Telephone Number	Home telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Mobile Telephone Number	Mobile telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Contact Telephone Number	Contact telephone number of user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.

Field	Description	Remarks
Alternative Telephone Number	Alternative telephone number for user	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Email Address	User email address	Best Practice: Although not a mandatory field, it is useful to set up users with their correct email addresses.
Job Title	Job title of user	-
Directory Filter		-
Information	Additional Information for user	-
Misc		-
Welcome Message		-
Extra 1		-
Extra 2		-
Extra 3		-
Extra 4		-

Step 4 After completing the relevant fields on this page, click the Next button.

Note: Required fields are indicated by a red asterisk (*).

Step 5 Complete the required fields and click the **Add** button, the user account will be added to the database.

Field	Description	Remarks
GUI Branding	The branding theme (colors, fonts, items look & feel etc.) to display to the user when they log into the system.	Select the required presentation theme from the drop-down list. The branding themes are defined by the Provider administrator. The applicable branding themes should be enabled for each level in the system hierarchy.
Preferred Country	The country to which the administration user will be linked.	Select from the drop-down list.
Access Profile	Defines the system's menu options available for the user.	This is a mandatory field. Select from the drop-down list. Default access profile is provided as part of the product. The available access profiles are defined by the Provider Administrator.
Security Profile	The security profile.	Select the required security profile from the drop-down list.
Account number to use in external accounting system	The account number of the external accounting system.	Relevant only if you are using an external accounting system, enter the account number here.

Modifying an Administrator

Procedure

To modify an administrator:

- Step 1** Browse to *General Administration > Administration Users* .
 - Step 2** Select the *Username* (active text link) that you would like to modify.
 - Step 3** Make the required changes to the user's details and click the **Modify** button. The administrator will now be updated in the system.
-

Note

Administrators can only modify the details of another administrator at a level lower than their own level in the administration hierarchy.

Reset an Administrator's Password

Procedure

This process would be used for a User that has forgotten their Password:

- Step 1** Once you have found and selected the required user, you will need to access the Password screen by clicking the Change Password button.
 - Step 2** Enter a new Password and verify it by re-entering it and clicking the Submit button.
-

Note

You do not need to know the old Password, as this is a reset function. You only require a new or default Password.

Once the user logs into the system with the new password, the system will ask the user to change their password.

Deleting an Administrator

Procedure

To delete an administrator:

- Step 1** Browse to *General Administration > Administration Users* .
 - Step 2** Select the *Username* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button. The administrator will now be deleted from the system.
-



CHAPTER 5

Customer Administration

Customer Management	700
Add a Customer	701
View and Modify a Customer	703
Advanced Customer Management	703
Advanced Telephony Settings	704
Customer License Management	708
Preferences	710
Deleting a Customer	711
Copying Feature Groups	712
Activate User Roaming	712
Activate User Roaming via Preferences	712
Activate user extension mobility via feature groups	713
Activate user extension mobility for customers	713
Overview of Extension Mobility Cross Cluster for Customers	714

Customer Management

The customer in the system represents the organization/company that is purchasing the telephony service. Each customer may have one or more locations defined, and it is these that actually are provided with the telephony service. Administrators maybe created for each customer enabling customers to potentially administer their own telephony services i.e. Perform their own Adds, Move and modifications, although at the discretion of the service provider or reseller.

Note

It is faster to use bulk loading if you have more than one customer to add, see the Bulk Loaders documentation for more information.

The following tasks will need to be performed for a customer to successfully provision the system.

Note

The majority of these steps will be completed via the bulk data loaders.

Overview of Provisioning a Customer

- At the Provider Level
 - Task 1: Create a customer and allocate phones to the inventory.
- At the Customer Level
 - Task 2: Create a division(s) (if needed), location(s), and tenant(s).

Task 3: Create feature groups.

Task 4: Move phones to the required location.

- At Location Level

Task 5: Create the relevant users for each location.

Task 6: Register the phones and associate them with the relevant users.

Note

For more information on location administration, refer to [Managing a Location on page 757](#).

Add a Customer

The Customer in the system represents the organization/company that is purchasing the telephony service. Each Customer may have one or more Locations defined, and it is these that actually are provided with the telephony service. Administrators maybe created for each Customer enabling customers to potentially administer their own telephony services i.e. Perform their own Adds, Move and Changes, although at the discretion of the Service Provider or Reseller.

Note

It is faster to use Bulk Loading if you have more than one customer to add, see the Bulk Loader Guide for more information.

Procedure

To add a customer:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields. The following fields are available when adding a customer:

Fields	Description
Details:	
Name	The name of the Customer being added. The name must be unique, and is a mandatory field.
Extended Customer Name	An optional field for expanding on the customer's name.
External Customer ID	This field enables an external system to map a Customer ID to an external customer ID. For example, if the customer ID is <i>Customer_123</i> but an organizations billing system uses a customer reference of <i>London_South_Site-123</i> , the <i>External Customer ID</i> field can be specified as <i>London_South_Site-123</i> . This is an optional field and is limited to a maximum of 100 characters. This field must be unique within the Provider/Reseller/Customer realm.
Address1	Address field 1 of the customer.
Address2	Address field 2 of the customer.
Address3	Address field 3 of the customer.
City	City where the customer is located.
State	State where the customer is located.

Fields	Description
Country	Country where the customer is located. This is a mandatory field. Select from the drop-down list, default = the country of the reseller to which the customer is being added
Post/ZIP Code	Post/ZIP Code where the customer is located.
Contact Name	Contact Name of the person responsible for the customer.
Telephone Number	Telephone number for the person responsible for the customer.
Contact Email	Email address for the person responsible for the customer.
Account number to use in external accounting system	The relevant account number to use for any billing transactions related to the customer.
Security Profile	The security profile related to the customer. Options include security profiles that have been configured for your system as well as the <i>None</i> and <i>Default</i> options.
User Group	<p>Specify a user group for the customer.</p> <p>This user group is combined with the username of each user created at Customer level to ensure a unique username.</p> <p>Note</p> <ul style="list-style-type: none"> • This field is available in system version 8.0 and higher, and only to System, Provider and Reseller administrators. • If the user group of a customer is modified or deleted, the changes are reflected in the username of these users. • Spaces are not allowed in user group names.
Provided Services Details:	
IP Address	The IP address of the customer. If this is not configured, it defaults to the system cluster's virtual IP Address.
Dial Plan Details:	
Inter-Site Prefix	The Inter-Site prefix for this customer.
Site Code Rules	The Site code rules for this customer, for example Max 5 digits.
Site Code	The Site code for this customer.
Last Site Code in range (optional)	The last site code in range for this customer (if you wish to provision a range of site codes). If this field is not completed, only one site code is provisioned (as specified in the above field).
GUI Branding	
Default branding of User Interface	Select the default GUI branding interface related to the customer from the drop-down list.
Default GUI branding	Select the checkbox to apply the required default GUI theme for this customer.
Button Groups	
The Button Groups related to the customer.	
Phone Button Template Group default	The Phone Button Template Group default related to the customer.
Softkey Template Group	The Softkey Template group related to the customer.

Fields	Description
Codecs	
Enable Location Codec Configurable	Select the checkbox if required.
Intra-Region Max Audio Bit Rate	Select from the drop-down list the Intra-Region Max Audio Bit Rate to be applied to the customer.
Inter-Region Max Audio Bit Rate	Select from the drop-down list the Inter-Region Max Audio Bit Rate to be applied to the customer.
	Note Codecs can only be set at the customer/building level, if the associated dial plan makes provision for it.

- Step 4** Click the **Add** button when complete. The customer is created in the system.

View and Modify a Customer

The Customer in the system represents the organization/company that is purchasing the telephony service. Each Customer may have one or more Locations defined, and it is these that actually are provided with the telephony service. Administrators maybe created for each Customer enabling customers to potentially administer their own telephony services i.e. Perform their own Adds, Move and Changes, although at the discretion of the Service Provider or Reseller.

Procedure

Modify Customers

To modify the settings of a customer:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the Customer *Name* (active text link) that you would like to modify.
- Step 3** Make the required changes to the customer. The following fields are as for [Add a Customer on page 701](#).
- Step 4** Click the **Modify** button when complete. The customer is updated in the system.

Procedure

Delete a Customer

To delete a customer:

- Step 1** Browser to *General Administration > Customers*.
- Step 2** Select the Customer *Name* (active text link) that you would like to delete.
- Step 3** Click the **Delete** button. After confirming the deletion, the customer is removed from the system.

Advanced Customer Management

Procedure

To manage advanced Customer configuration settings:

- Step 1** Browse to *General Administration > Customers*.
 - Step 2** Select the Customer *Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the relevant button associated with the type of configuration settings you want to manage. Available options are:
 - View PGW Config
 - Advanced Telephony Settings
 - License Management
 - Hardware Group Association
 - CLI Group Management
-

Advanced Telephony Settings

This screen consists of a list of available advanced telephony features. Currently, the available settings include:

- FwdRedirectingExternalNumonCallFwd
- Block Offnet to Offnet Transfer
- Post Dial Delay Bypass
- Emergency CLI Preference
- Default SNR Rerouting CoS
- Allow CoS per SNR Profile

FwdRedirectingExternalNumonCallFwd

The *FwdRedirectingExternalNumonCallFwd* setting is used to manage the *AssociateFNN-Redirect* and *DisassociateFNN-Redirect* transactions at the customer level. This setting drives the use of the AssociateFNN-Redirect model. The purpose of the feature and model is to include a mapping in the TimesTen DB for calls being forwarded to the PSTN. In the case where the calling number matches an entry, its FNN would be used as the CLI for the call (instead of the default behavior of site published number).

The *DisassociateFNN-Redirect* setting is managed via a drop-down list. The following options are available from the drop-down list:

- Derived From Provider: This is the default setting. This setting is enabled or disabled based on the setting at the Provider level.
- Enabled: Regardless of the setting at the Provider level, this feature is enabled for the Location.
- Disabled: Regardless of the setting at the Provider level, this feature is disabled for the Location.

Procedure

Modifying the Setting

To modify the status of the *AssociateFNN-Redirect* setting:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the Customer *Name* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Advanced Telephony Settings** button.
- Step 5** Select the required status from the drop-down list.
- Step 6** Click the **Apply** button. After confirming the operation, the AssociateFNN-Redirect transaction is activated.
-

Block Offnet to Offnet Transfer

The *Block Offnet to Offnet Transfer* setting is used to manage the *Block Offnet to Offnet Transfer* behavior at the customer level.

The *Block Offnet to Offnet Transfer* setting can either be enabled or disabled:

- Enabled: Offnet to Offnet transfers is blocked at the customer level.
- Disabled: Offnet to Offnet transfers are not blocked at the customer level.

Procedure

Modifying the Setting

To modify the *Block Offnet to Offnet Transfer* setting:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the Customer *Name* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Advanced Telephony Settings** button.
- Step 5** Click the required button adjacent to the *Block Offnet to Offnet Transfer* option, either **Enable** or **Disable**.
-

The *Block Offnet to Offnet Transfer* status is updated.

Post Dial Delay Bypass

To accommodate variable length numbers, Cisco Unified Communications Manager (Unified CM) usually waits for a timeout to expire before considering a number complete. The *Post Dial Delay Bypass* feature enables providers to distribute fixed length route patterns to Unified CM clusters so that, when numbers corresponding to these patterns are dialed, the connection is made immediately, rather than waiting for the timeout.

It is important to first understand what happens when locations are added, in order to understand the *Post Dial Delay Bypass* setting.

Adding the first location to a server

When a location is added, the *AddLocation* transaction is initiated, which checks whether the location being added is the first for the current customer on the current IPPBX, and if so, adds the *CustomerWide* partition by calling the *PostDialDelayPartition* model. This happens, irrespective of whether the customer's Post Dial Delay Bypass is enabled or disabled. The *AddLocation*

transaction also calls the *RegisterPhone* model to create a set of Calling Search Spaces (and associated CoS names) which includes the new *CustomerWide* partition.

Adding new locations

Every time a new location is deployed, the target IPPBX is checked to determine how many locations, which are associated with the Customer of the new location being added, currently exist. This indicates whether the Post Dial Delay Bypass route patterns for all the other locations have been added to this server for the specified customer. If these route patterns do not already exist, route patterns are created. The *AddLocation* transaction triggers the *AddLocationICTSiteCodesCust* model to achieve this.

AddLocationICTSiteCodesCust will:

- Add a route pattern for this location to the *CustomerWide* partition.
- Add the route pattern to the *CustomerWide* partition on all other servers for the current customer.
- Add the route patterns for all other locations for the current customer on other servers to the *CustomerWide* partition on these servers.

Modifying the Post Dial Delay Setting

The *Post Dial Delay Bypass* setting can either be enabled or disabled:

- Enabled: The delay which is normally experienced after dialing and before a call is connected is **not** experienced.
- Disabled: The delay which is normally experienced after dialing and before a call is connected **is** experienced, as determined by Cisco Unified Communications Manager.

Procedure

To modify the *Post Dial Delay Bypass* setting:

On clicking the *Enable* button, the following back-end transaction is triggered:

- *EnablePostDialDelay*, which adds the new *CustomerWide* partition and related CSS's which will apply to the Customer and its locations. It also creates the route patterns for each location connected to each associated customer device.

On clicking the **Disable** button, the following back-end transaction is triggered:

- *DisablePostDialDelay*, which removes the route patterns for each location connected to each associated customer device.

- | | |
|---------------|--|
| Step 1 | Browse to <i>General Administration > Customers</i> . |
| Step 2 | Select the <i>Customer Name</i> (active text link) that you would like to modify. |
| Step 3 | Click the Advanced Mgt. button. |
| Step 4 | Click the Advanced Telephony Settings button. |
| Step 5 | Click the required button adjacent to the <i>Post Dial Delay Bypass</i> option, either <i>Enable</i> or <i>Disable</i> . |
-

Deleting a location with Post Dial Delay bypass disabled

The *DeleteLocation* transaction is called. Regardless of whether or not *Post Dial Delay* is enabled, if the location being deleted is the last location for the current customer on the server, the *CustomerWide* partition is deleted. Route patterns are not affected.

Deleting a location with Post Dial Delay bypass enabled

The *DeleteLocation* transaction is called, which removes the route pattern for the current location from the *CustomerWide* partition, on the current and all other servers on which locations for the current customer exist.

Emergency CLI Preference

The *Emergency CLI Preference* is used to manage the *Emergency CLI* behavior at the customer level.

The *Emergency CLI Preference* setting is managed via a drop-down list. The following options are available from the drop-down list:

- Emergency Number: The preference uses the Emergency Number.
- Device CLI: The preference uses the Device CLI.

Procedure

Modifying the Setting

To modify the *Emergency CLI Preference* setting:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the *Customer Name* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Advanced Telephony Settings** button.
- Step 5** Select the required status from the drop-down list adjacent to Emergency CLI Preference.
- Step 6** Click the **Apply** button. After confirming the operation, the Emergency CLI Preference is updated.

Route patterns pointing at a new site will be # *ISP* double# *SiteCode* # *XXXX* depending on the configured extension length for the new Location (i.e. the *XXXX* part is variable according to extension length).

For more information on models refer to the *Call Manager Model Guide*.

Default SNR Rerouting CoS

The *Default SNR Rerouting CoS* setting is used to allow a customer to configure the SNR Rerouting CSS.

This setting must be configured, that is an option **must be selected** from the drop-down list in order to configure the *Allow CoS per SNR Profile* setting (see below).

Available values are the 'outbound' service types configured for the dialplan. Select an option from the drop-down list and click the adjacent **Modify** button when complete.

Allow CoS per SNR Profile

The *Allow CoS per SNR Profile* setting allows for two separate modes of control for the SNR rerouting CSS:

- With CoS-per-profile **disabled** (default setting) at the customer level, the SNR rerouting CoS is controlled via values set per location and per customer. The existing dialplan default CSS is applied if these values are not set.

- With CoS-per-profile **enabled** for a customer, each individual SNR profile (end user) can individually configure the CoS value.

Note

This setting cannot be enabled if there are existing SNR profiles for this customer that are using the dialplan global CSS.

The *Default SNR Rerouting CoS* setting (see above) must be configured to use this setting.

Click the **Disable** or **Enable** button as required.

Customer License Management

The *Customer License Management* page enables providers to manage the licenses and billing of their customers. The three key tasks that providers can carry out on this page include:

- Enabling of OSS/BSS License Modules for Customers
- Association of License/Service Types to Customers
- Association of Language Licenses to Customers

The system caters for the following licensing scenarios:

- Customers are billed based on licenses and license usage is tracked in the system and customers have the ability to purchase and update their own licenses for a location in the system.
- Customers are billed based on licenses and license usage is tracked in the system. However, a customer does not have the ability to purchase and update their own licenses for a location in the system.

Procedure

Enabling of OSS/BSS License Modules for Customers

Follow the steps below to enable license modules for customers:

- Step 1** Navigate to *General Administration > Customers*
- Step 2** Select the **Advanced Management** button
- Step 3** Select the **License Management** button
- Step 4** Select the required checkboxes within the *Enable OSS/BSS License Module for Customer* section

The following options are available:

- General License Management
- License Management GUI

Note: You are not able to select any modules unless the *General License Management* module is selected.

- Step 5** Select the **Modify** button

The selected modules will be enabled for the selected customer.

Procedure

Disabling of OSS/BSS License Modules for Customers

Follow the steps below to disable license modules for customers:

- Step 1** Navigate to *General Administration > Customers*
- Step 2** Select the **Advanced Management** button
- Step 3** Select the **License Management** button
- Step 4** Deselect the required checkboxes within the *Enable OSS/BSS License Module for Customer* section
- Note:** You are not able to deselect the *General License Module* while other modules are still selected.
- Step 5** Select the **Modify** button

The selected modules will be disabled for the selected customer.

Procedure

Association of License/Service Types to Customers

Note: You are not able to select any Services/License Types unless *General License Module* is selected within the *Enable OSS/BSS License Module for Customer* section.

Follow the steps below:

- Step 1** Navigate to *General Administration > Customers*
- Step 2** Select the **Advanced Management** button
- Step 3** Select the **License Management** button
- Step 4** Select the checkbox(s) adjacent to the required *Services/License Type(s)*
- Step 5** If required, select the **Billing** checkbox(s) adjacent to the relevant *Services/License Type(s)*
- Step 6** Select the **Modify** button

The selected Services/License Type(s) will be enabled for the selected customer.

Procedure

Dissociation of License/Service Types to Customers

Follow the steps below:

- Step 1** Navigate to *General Administration > Customers*
- Step 2** Select the **Advanced Management** button
- Step 3** Select the **License Management** button
- Step 4** Select the checkbox(s) adjacent to the required *Services/License Type(s)*
- Step 5** Select the **Modify** button

The selected Services/License Type(s) will be disabled for the selected customer.

Procedure

Association of Language License to Customers

Follow the steps below:

- Step 1** Navigate to *General Administration > Customers*
- Step 2** Select the **Advanced Management** button
- Step 3** Select the **License Management** button
- Step 4** Select the required languages from the *Available Languages* list

Notes:

- English (United States) will always appear in the *Available Languages* list
- The first language on the *Selected Languages* list will be the default language for the customer. (To the right of the selected languages select box are two buttons for re-ordering the selected languages. The only significance of the order is that the top language in the selected languages box will be used as the default language for the Customer.)
- The customer's default language can be overridden by an end user's browser language or by another licensed language selected for or by the end user. When a language has been selected for an end user, this language overrides the customer's default language, as well as the language set in the browser. When no language has been selected for an end user, the browser's language will be used if that language has been licensed to the Customer of the end user. However, if the browser language is not licensed then the customer's default language will be used.

Preferences

Procedure

To manage a Customer's preferences and settings:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the *Customer Name* (active text link) that you would like to modify.
- Step 3** Click the **Preferences** button. The *Preferences and Settings: Customer* screen is displayed listing the preferences and settings available to the customer. See the table below for a list and description (if necessary) of each preference or setting. See also [Customer Preference and Settings on page 942](#) for more details.
- Step 4** Click the relevant *Name* (active text link) to view the status.
- Step 5** Change the status if required by selecting/unselecting the associated checkbox, or by modifying the existing text field, and then clicking the **Modify** button.

Field	Description
AllowCrossClusterLogin	Allows a roaming user to login across locations.
AllowRoamingMultiLogin	Allows a roaming user to login to multiple phones simultaneously. This is restricted to phones within the same cluster.
AllowSelfCarePINResetNoPrevious	Allows Self Care End User to reset their Voicemail and Extension Mobility Pin without having to provide the previous Pin.
AutoFeatureCustomer	Feature Group for Phone based registration (unless overridden by Location preference).
AutoLastResortFeatureCustomer	Feature Group for Last Resort Phones (unless over-ridden by Location preference).

Field	Description
AutoMoveCustomer	Allows Auto Move of Phone to locations (unless over-ridden by Location preference).
AutoRegisterLowestCustomer	Lowest allowed extension number for Phone based Auto registration (unless over-ridden by Location preference).
CustomerDefaultLoginPassword	Use the default password to reset user passwords.
EnableUniquenessIndicator	Enable Uniqueness to naming of IPT entities. If this setting is enabled, the Location ID is appended to the device pool name for a 'Custom' device pool. The setting is named generically to allow future uniqueness indicators to use the same preference setting.
EndUserNamesAllNumeric	User Name required all numeric.
ForceOldRoamingLogoff	Force Roaming logoff (on old phone) if user logs in elsewhere.
HuntGroupCallFwdCOS	COS to be used when setting Call forward for Hunt groups.
PerLineCallFwdCoS	Allows Call Limitations to be applied per Line for forwarded calls.
RoleLoginRequirePIN	Require entry of PIN during Role Login style Auto Registration.
ShowCorporateDir	Display Corporate Directory on phones.
ShowCorporateDir-Unreg	Display Corporate Directory on Unregistered phones.
ShowPersonalDir	Display Personal Directory on phones.
ShowSpeedDials	Display SpeedDials on phone.
UniqueEndUserEmailRequired	Ensures that end users have a valid and unique email address.
UseUserNameAsVMBoxNum	Use UserName as voicemail box number.
XML-CallForwardAll	Allow CallForwardAll editing via Services Menu.
XML-CallForwardBusy	Allow CallForwardBusy editing via Services Menu.
XML-CallForwardNoAnswer	Allow CallForwardNoAnswer editing via Services Menu.
XML-DirDisplayForLocalLocation	Rule to use for displaying Directory Numbers for Users in the Local Location.
XML-DirDisplayForRemoteLocation	Rule to use for displaying Directory Numbers for Users in the Remote Location.
XML-PhoneAutoRegistration	Display Phone Auto Registration option on Services Menu.
XML-PhoneBasedLanguageSelection	Display Phone Based Language Selection option on Services Menu.
XML-PhoneBasedProvisioning	Display Phone Based Provisioning option on Services Menu.
XML-PhoneLastResort	Display Phone Last Resort option on Services Menu.
XML-RoleLoginRegistration	Display Phone PIN Registration option on Services Menu.
XML-SetCallFwdPerLine	Allow CallForward settings to be applied per Line.

Deleting a Customer

Procedure

To delete a customer:

- Step 1** Browse to *General Administration > Customers*.
 - Step 2** Select the *Customer Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button. After confirming the deletion, the customer is removed from the system.
-

Copying Feature Groups

Note

For more information on feature groups, refer to *Feature Group Administration* in the Deployment Guide.

Procedure

To copy a feature group for a location:

- Step 1** Browse to *General Administration > Feature Groups*.
 - Step 2** Make sure you are in the location that you would like to manage.
 - Step 3** Click the **Create From Template** button.
 - Step 4** Enter a *New Name* adjacent to the group you would like to copy then click the **Create From Template** button.
-

The feature group is copied and then added to the location.

The following are available when copying a feature group:

Field	Description	Remarks
Copy From Template	Button allowing copy for the Feature Template.	-
Name	Name of Feature Template	-
Description	Feature Template description	-
New Name	The name for the Feature Group at the customer level once copied from the Feature Template.	This is a mandatory field.

Activate User Roaming

The activation via preferences and feature groups is covered as well as user roaming and cross-cluster roaming.

Activate User Roaming via Preferences

To activate the user roaming feature:

Note

When using the Cisco Unified Communications Manager (Unified CM) Login/Logout Service, as opposed to the system's (CUCDM's) Roaming Login/Logout

Service, ensure that the *BVSMUserRoaming* preference option is **not** selected (deactivated), since these two services are mutually exclusive.

Procedure

- Step 1** Browse to *Provider Administration > Providers*.
- Step 2** Select the relevant *Provider* (active text link).
- Step 3** Click the **Preferences** button.
- Step 4** Select the *BVSMUserRoaming* (active text link) preference.
- Step 5** Select the checkbox, and then click the **Modify** button. User roaming is activated within the system.

Activate user extension mobility via feature groups

Note

Do not activate the *Allow User login to Phone* option if there are phones within the feature group that do not support extension mobility.

Procedure

To activate user extension mobility via feature groups:

- Step 1** Browse to *General Administration > Feature Groups*.
- Step 2** Select the required *feature group* (active text link).
- Step 3** Ensure that the *User Mobility* and *Allow User login to Phone* checkboxes are selected (enabled), and then click the **Modify** button. User roaming is activated within the system.

Activate user extension mobility for customers

Procedure

To activate user roaming for customers:

- Step 1** Browse to *General Administration > Customers*.
- Step 2** Select the relevant *customer* (active text link).
- Step 3** Click the **Preferences** button.
- Step 4** Select the *AllowCrossClusterLogin* active text link.
- Step 5** Select the checkbox to enable the setting then click the **Modify** button.
- Step 6** Select the *Return to Preferences Management* active text link.
- Step 7** Select the *ForceOldRoamingLogoff* active text link.
- Step 8** Select the checkbox then click the **Modify** button. User extension mobility is activated within the system.

Overview of Extension Mobility Cross Cluster for Customers

Note

Only **ONE** method of cross cluster roaming can be used, i.e., the standard cross cluster roaming feature (method 1) and the extension mobility cross cluster feature (method 2) can **NOT** be activated at the same time. The preferred option is Method 2 (see [Extension Mobility Cross Cluster \(EMCC\) - Method 2 on page 714](#)).

Standard Extension Mobility Cross Cluster - Method 1

If the customer preference *AllowCrossClusterLogin* is enabled for Cross Cluster Mobility, and a user with a roaming profile on cluster1 tries to login to a phone registered on cluster 2, the following will occur:

- The system sets the user's roaming profile settings *CallForwardNoAnswer* and *CallForwardNotRegistered* to the diallable number for the first line of the Phone. This will enable all calls to the user to be forwarded to the phone they log into.
- No user profile is created on the 2nd cluster and the phone retains its existing line and COS settings while the user uses it.
- The number sent for outcalls is the number for the line of the phone instead of the user's line number.

The impact on the user's available features and experience is as follows:

- Line settings: Phone retains its lines and existing settings (including DDI, emergency call routing, etc.).
- Speed dials: The user sees their speed dials when using the system's XML app. Abbreviated dialing does not work as this relies on the speed dials being loaded against that phone in Unified CM.
- Personal directory: The user sees their personal directory.
- Callforward: Any changes to the *callforward* setting via the phone XML interface applies those setting to the user's profile and not the phone.
- Voicemail: Voicemail uses the phones assigned pilot number. The user needs to login as the number passed during the call is not theirs. Calls forwarded to voicemail do not go to the correct mailbox.

See also: [Extension Mobility Cross Cluster \(EMCC\) - Method 2 on page 714](#) - Method 2.

Extension Mobility Cross Cluster (EMCC) - Method 2

The Extension Mobility Cross Cluster feature (EMCC) feature extends the existing mobility feature (roaming profile) within a single cluster to operate across multiple Cisco Unified Communications Manager (Unified CM) clusters. EMCC allows a user of one Unified CM cluster (the home cluster) to log in to an IP Phone of another Unified CM cluster (the visiting cluster) during travel as if the user is using the IP phone at their home site.

Procedure

To enable the EMCC feature at the customer level:

- Step 1** Make sure that the customer preference *AllowCrossClusterLogin* configuration setting used in Method 1 is *disabled* (switched *OFF*).

-
- Step 2** Browse to *Provider Administration > Providers*.
- Step 3** Select the required *Provider Name* (active text link). The *Manage Service Provider* screen is displayed.
- Step 4** Click the **Preferences** button. The *Preference and Settings: Provider* screen is displayed.
- Step 5** Select the *BVSMUserRoaming* link (active text link). The *Preference and Settings* screen is displayed.
- Step 6** Make sure that the *BVSMUserRoaming* checkbox is *disabled (NOT selected)*. Confirm this by clicking the **Modify** button if required.
- Step 7** Browse to *General Administration > Feature Groups*.
- Step 8** Select the required *Customer Name* (active text link) if required.
- Step 9** Select the required feature group *Name* (active text link). The *Manage Feature Group* screen is displayed.
- Step 10** Select (*enable*) the following checkboxes:
1. User mobility (under User)
 2. Allow user login to phone (under Handset)
 3. Extension Mobility Cross Cluster (under Value Add)
- Step 11** Browse to *General Tools > Operations Tools*.
- Step 12** Select the required *Provider Name* (active text link). The *Operations Department Tools* screen is displayed.
- Step 13** Re-apply the feature group settings on the devices and users as required by running the appropriate Ops tools by selecting the active text link (see below):
- Re-apply feature group capabilities for a given location
 - Re-apply feature group capabilities for a given division
 - Re-apply feature group capabilities for a given customer
- Step 14** Upon completion, the feature groups assigned to all users and phones in the location/division/customer are re-applied to the user's roaming profiles and the phones.
-

Note

If the *BVSMUserRoaming* option is selected (*enabled*), then only the normal Extension Mobility capability is available irrespective of the *Extension Mobility Cross Cluster* setting.

In addition to the configuration settings described above, EMCC requires the relevant location to have an associated GeoLocation as described under [Geolocation Management on page 405](#).

Once EMCC is correctly configured and enabled, and a user with a roaming profile on cluster 1 tries to login to a phone registered on cluster 2, the user's phone does not display a Login/Logout option on the *Services* menu instead of the *Roaming Login/Logout* option. After selecting the *Login* option, all phone features that were available on the device in cluster 1 are now available on the device in cluster 2 (if supported by the device).

See also: [Extension Mobility Cross Cluster \(EMCC\) Configuration on page 401](#).



CHAPTER 6

Division Administration

[Add a Division](#) 716

[Modifying a Division](#) 717

Divisions are used to group locations and are aimed at large Enterprises, or Tenants, with many Locations. The grouping of Locations into Divisions allows for easier, day to day management, rather than a Customer Administrator having to search through 10s or 100s of locations.

If you are an Administrator with the correct authority, you will only need to add a Division when your organization opens a number of new sites or branches and there is a need to create a new group of Locations.

Note

You do not need a new Division for every Location, but each Customer must have at least one Division to add a Location.

Add a Division

This section describes how a Customer Administrator (or higher) is able to create a new Division within the system. Divisions are used to group locations and are aimed at large Enterprises, or Tenants, with many Locations. The grouping of Locations into Divisions allows for easier, day to day management, rather than a Customer Administrator having to search through 10s or 100s of locations.

If you are an Administrator with the correct authority, you will only need to add a Division when your organization opens a number of new sites or branches and there is a need to create a new group of Locations.

Note

You do not need a new Division for every Location, but each Customer must have at least 1 Division to add a Location.

Procedure

To add a new division:

Step 1 Select *Divisions* under the *General Administration* Menu.

Note

A Division Administrator cannot add a new Division. Only Customer Administrators (or higher) are authorized to add Divisions.

Step 2 **Note**

If you have Administration status higher than Customer Administration, then to get to the Division Management page, you may be required to select Provider, Reseller and Customer, before you can access Division.

Click the **Add** button on the *Division Management* screen. The *Add Division* screen is displayed.

Step 3 Complete all of the required details. Available fields include:

Attribute	Description
Details:	
Name	Name of the division, for example, "West London". This is a mandatory field.
Extended Division Name	Extended or custom name of the division, for example "Twickenham to Reading".
Address1	Primary address field for division. This is a mandatory field.
Address2	Secondary address field (if required) for division.
Address3	Third address field (if required) for division.
City	City where division is located. This is a mandatory field.
State	State where division is located.
Country	Country where division is located. This is a mandatory field. Select from the drop-down list, default = the country of the customer to which the division is being added.
Post/ZIP Code	Post/ZIP code where division is located. This is a mandatory field.
Contact Name	Primary contact person for division. This is a mandatory field.
Telephone Number	Telephone number for primary contact person for division. This is a mandatory field.
Contact Email	Email address for primary contact person for division
Account number to use in external accounting system	The number to be used to identify the division if an external accounting system is being used.
Security Profile	The security profile to be used for the division.
Directory Partition	Select the required directory partition from the drop-down list. The available directory partitions are defined by the administrators at the different levels of the hierarchy.
GUI Branding:	
Default branding of User Interface	Select the default branding for the division. The branding option is selected from the drop-down list.
Default GUI branding	Selects whether default GUI branding is enforced. Select the check-box to enforce or deselect the check-box to not enforce.

Step 4 Click the **Add** button when complete. The system creates the new Division.

Modifying a Division

This section describes how a Customer Administrator (or higher) is able to manage and delete a Division within the system.

Procedure

Modification of a Division's details will be required whenever changes occur. To modify a division:

Step 1 Browse to *Divisions* under the *General Administration* Menu.

Note: A Division Administrator cannot add a new Division. Only Customer Administrators (or higher) are authorized to add Divisions.

Note: If you have Administration status higher than Customer Administration, then to get to the Division Management page, you may be required to select Provider, Reseller and Customer, before you can access Division.

Step 2 Select the relevant Division *Name* (active text link) from the *Division Management* screen that you would like to modify. The *Division Management* screen is displayed.

Step 3 Modify the fields as required.

Step 4 Click the **Modify** button when complete to save your changes. The changes made to the division will be saved to the system.

If you are an Administrator with the correct authority, you will need to delete a Division when your organization closes all sites or branches in the Division and needs to shut down your IP telephony system into the Division.

Procedure

To delete a division:

Step 1 Browse to *Divisions* under the *General Administration* Menu.

Note: A Division Administrator cannot add a new Division. Only Customer Administrators (or higher) are authorized to add Divisions.

Step 2 **Note:** If you have Administration status higher than Customer Administration, then to get to the Division Management page, you may be required to select Provider, Reseller and Customer, before you can access Division.

Select the relevant Division *Name* (active text link) that you wish to delete.

Step 3 Click the **Delete** button. After confirming the delete operation, the division will be deleted from the system.

Note: You cannot delete a Division while there are Locations within that Division. Locations must be deleted before a Division can be deleted.

Procedure

Add an Area Code

Before you can create an inventory of E164 numbers, you must configure area codes and have a range of numbers allocated to the area codes.

To add an area code:

Step 1 Browse to *Resources > E164 Inventory* .

Step 2 Select a country to which you would like to add an area code then click the Next button.

- Step 3** Click the Area Code Mgt button.
- Step 4** Click the Add button.
- Step 5** Enter the required area code and click the Add button. The area code will be added to the system.

Note

- This procedure needs to be repeated for all required area codes.
 - The same area code can exist across different customers and only once per reseller.
 - The administrator user will not be able to add codes that exist at a level higher than the level he belongs to, e.g. a customer administrator cannot add a code that already exists for his Reseller or Provider.
-

Procedure

To manage existing area codes:

- Step 1** Browse to *Resources > E164 Inventory* .
- Step 2** Select a country to which you would like to add an area code then click the Next button.
- Step 3** Click the Area Code Mgt button.
- Step 4** Click the **Delete** button adjacent to the relevant area code.

Note

- Only area codes which are not in use by the E164 inventory can be deleted.
 - An administrator cannot delete area codes created by administrators of a higher hierarchy level.
 - The Manage Area Codes screen displays the hierarchy entity (Provider, Reseller, Customer) of the administrator who added the area code, as well as the other associated hierarchy entities.
-

Procedure

Add E164 Numbers

The system allows for the option to add a single E164 number or a range of numbers.

- Step 1** Follow steps under [Managing E164 Numbers on page 574](#) if required to get to the screen above. On the E164 list page, click the Add Number button.
- Step 2** Update the values for the new E164 number as required and click the Add button. The following fields are available:

Field	Notes	Remarks
Country	ISO country code and country name.	-

Field	Notes	Remarks
National Area Code	Area code prefix for the PSTN number.	By default the area code presented is the one to select while going through the steps getting to the E164 List. However, if the number to be added is of a different area code, the system allows it to be changed by selecting from the drop-down list. Notes: The system will automatically add the area code to the area codes list if it does not yet exist in the system. Even if the country dial plan requires a leading digit for calling with an area code, in this screen, it should be written without any leading digits.
Local Number	The E164 number in the area code.	-
Hardware Group	The hardware group to which this number will be added.	Select from a drop-down list. The available options match the hierarchy of the user adding the E164 number. The hardware group is used to allow the concept of control over which hardware is updated when transactions against this E164 number is run.
User Data	Each E164 inventory entry can be assigned a user data field. This enables operators to track E164 numbers against contractual requirements.	This is an optional field.

Procedure

Add E164 Number Range

To add an E164 Number Range:

- Step 1** Follow steps under [Managing E164 Numbers on page 574](#) if required to get to the screen above. On the E164 list page, click the Add Number Range button.
- Step 2** Update the values for the new E164 number range as required and click the Add button. The following fields are available:

Field	Description	Remarks
Country	ISO country code and country name.	-

Field	Description	Remarks
National area code	Area code prefix for the PSTN number.	<p>By default the area code presented is the one to select while going through the steps getting to the E164 List. However, if the number to be added is of a different area code, the system allows it to be changed.</p> <p>Notes:</p> <p>The system will automatically add the area code to the area codes list if it does not yet exist in the system.</p> <p>Even if the country dial plan requires a leading digit for calling with an area code, in this screen, it should be written without any leading digits.</p>
Start of number range	The first number in the required range.	-
End of number range	The last number in the required range.	-
Hardware Group	The hardware group to which these numbers will be added.	<p>Select from the drop-down list.</p> <p>The hardware group is used to allow the concept of control over which hardware is updated when transactions against the E164 numbers are run.</p>
User Data	Each E164 inventory entry can be assigned a user data field. This enables operators to track E164 numbers against contractual requirements.	<p>This is an optional field.</p> <p>The value supplied in the User Data field will be applied to all of the numbers within the range.</p>

See also: [Managing E164 Numbers on page 574](#).



CHAPTER 7

Building Administration

Managing Buildings 722

Adding a Building 723

Managing Buildings 724

Site Code Management for Buildings 727

Managing Building Voicemail Services 728

Voicemail Pilot Number Management 730

Selecting the Required Voicemail Service Profile 731

Manage Building Auto Attendant Services 732

Allocating E164 Numbers to the Voicemail and Auto Attendant Services 732

Feature Group Management 734

Customer Building Management 736

Manage Building Preferences 739

Managing a Building Preferences and Settings 739

Managing a Building's Details 739

Allocating an E164 Number Inventory to a Building (Location) 739

Allocating a Phone to a Building (Location) 740

Building Voicemail Service - E164 Number Management 740

Adding an Emergency Published Number 742

Assigning an E164 Number Range to Internal Numbers 742

Managing Users and Phones 743

Operations Tools 743

Managing Buildings

The system has the ability to manage buildings and areas within buildings. Equipment is always physically located in an area. Areas are just arbitrary named groups of equipment that need to be considered as being 'together'. For example, three rooms in a building that are all connected to the same router can be nicely grouped as an 'area' (even if they are not on the same floor).

The system can use the area groupings to make useful decisions on who should be allowed to manage a set of devices. Typically, a provider could manage a number of buildings and then a provider administrator role may be created, then restricted to managing the infrastructure in a particular building, or in a large building, perhaps just a few areas associated with some floors of equipment that they are responsible for.

Beyond the basic groupings of building and area, the system needs to also manage the relationships between these items, and the other assorted major business entities it understands: devices, resellers, customers, divisions, locations and people. For example, a building may be managed by a number of people, and any given person may manage a number of buildings. For example, a business location may exist in a number of areas of a building (or buildings), and a building may house a number of business locations (for a multiple resellers, customers or divisions too).

Note

You must be a service provider administrator, or higher, to manage buildings and to modify building details.

Adding a Building

Procedure

To add a new building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Click the **Add** button.
- Step 3** Complete the required fields. The following fields are available:

Field	Description
Building Name	The name of the building being added, for example "Main Wing" or "The John Smith building". This is a mandatory field.
Extended Building Name	Secondary name of the building, for example "admin block" or "main factory".
Address1	Primary Address for the Building.
Address2	Secondary address field for the Building.
Address3	Secondary address field for the Building.
City	City where building is located.
State	State where building is located.
Post/ZIP Code	Post/ZIP code where building is located.
Country	Country where building is located. This is a mandatory field.
TimeZone	Time zone in which the building is located or functions. This is a mandatory field.
Contact Name	Main contact person responsible for the building.
Telephone Number	Telephone number for the person responsible for the building.
Contact Email	Email address for the person responsible for the building.
IP Address	Corporate Directory Details.
Select a Hardware Group	The hardware group that the building will use. This is a mandatory field.

Field	Description
IPPBX	Select the required IPPBX from the drop-down list. This is a mandatory field.
Device Pool	Enter the device pool (if required).
IP Edge Device	<p>Note</p> <p>An IP Edge Device must have been created before attempting to assign it to a building.</p> <p>Select the required IP Edge Device (shareable across buildings) from the drop-down list. This is a mandatory field.</p>
Media Service Name	Select the required Media Service Name from the drop-down list.
Inter-Site Prefix	Select the required Inter-Site prefix from the drop-down list. This is a mandatory field.
External Access prefix	Select the required External Access prefix from the drop-down list. This is a mandatory field.
Building Access Code	Select the required Building Access code from the drop-down list. This is a mandatory field.
PBX Template	Select the required PBX Template from the drop-down list. This is a mandatory field.
Voice Bandwidth (Kbps)	Specify the required voice bandwidth in Kbps. This is a mandatory field.
Video WAN Bandwidth (Kbps)	Specify the required video bandwidth in Kbps. This is a mandatory field.
Codecs	
Intra-Region Max Audio Bit Rate	Select from the drop-down list the Intra-Region Max Audio Bit Rate to be applied to the building.
Inter-Region Max Audio Bit Rate	<p>Select from the drop-down list the Inter-Region Max Audio Bit Rate to be applied to the building.</p> <p>Note</p> <p>Codecs can only be set at the customer/building/location level, if the associated dial plan makes provision for it.</p>

Step 4 Click the **Add** button.

Managing Buildings

Procedure

Modifying a building

To modify a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the Building *Name* (active text link) that you would like to manage.
- Step 3** Modify the required fields and then click the **Modify** button. For available fields, refer to [Adding a Building on page 723](#). The buildings configuration is updated.

Advanced Building Modifications

From the *Manage Building* screen, a number of advanced modification options are available, these include:

Option	Description
Advanced Mgt	<p>The <i>Advanced Management</i> option launches a screen with the following advanced configuration options:</p> <ul style="list-style-type: none"> • Transit Switches on page 726 • CCM Device Pool Management on page 726 • Block Offnet to Offnet Transfer on page 705 <p>For more information, select the relevant link from the above list.</p>
Customers	<p>This option enables you to manage customers in relation to the building.</p> <p>For more information, see Customer Building Management on page 736.</p>
Voicemail	<p>This option enables you to manage voicemail services in relation to buildings.</p> <p>For more information, see Managing Building Voicemail Services on-page 728.</p>
Preferences	<p>From the preferences screen, the following options are available:</p> <ul style="list-style-type: none"> • Building Preferences • Default Customer Preferences • Default Location Preferences <p>For more information, see Building Preferences on page 949.</p>
Site Codes	<p>This option enables you to manage site codes in relation to buildings.</p> <p>For more information, see Site Code Management for Buildings on page 727.</p>
Feature Groups	<p>This option enables you to manage Feature groups in relation to buildings.</p> <p>For more information, see Feature Group Management on page 734.</p>
Auto Attendant	<p>This option enables you to manage Auto Attendant services in relation to buildings.</p> <p>For more information, see Manage Building Auto Attendant Services on-page 732.</p>

Deleting a Building

Procedure

To delete a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the building *Name* (active text link) of the building that you would like to delete.

- Step 3** Click the **Delete** button. After confirming the deletion operation, the building is removed from the system.
-

Transit Switches

Transit switches perform four main functions:

- Network inter-connectivity for signal processes (Ss7)
- Advanced routing capabilities for call control
- Regulatory Functions (911, Number Portability, etc.)
- Billing record generation

From the *Transit Switch* screen, you can view, but not modify, add or delete transit switches. A list displaying the transit switches currently configured is displayed, the information in this list includes *Name*, *Product* and *Description*.

Note

This screen **only** lists PGW transit switches. Other devices, such as Technician and SME, are not shown as configuration for these devices is not applied at this level.

To view further information for a transit switch, select the relevant Transit Switch *Name* (active text link). The details displayed include the *PGW Name*, *Dial Plan Type*, *Dial Plan Value*, *Customer*, *Division* and *Location*.

CCM Device Pool Management

[Adding a CCM Devicepool on page 727](#)

Procedure

Modifying a CCM Device Pool

To modify a device pool:

- Step 1** From the Advanced Building Management screen, click the **CCM Devicepool Management** button.
- Step 2** Select the Device Pool *Name* (active text link) that you would like to modify.
- Step 3** Modify the required fields and click the **Modify** button.
-

The device pool is modified within the system.

Procedure

Deleting a CCM Device Pool

To delete a device pool:

- Step 1** From the Advanced Building Management screen, click the **CCM Devicepool Management** button.
- Step 2** Select the Device Pool *Name* (active text link) that you would like to delete.
- Step 3** Click the **Delete** button.
-

The device pool is removed from the system.

Adding a CCM Devicepool

Procedure

To add a device pool:

- Step 1** From the Advanced Building Management screen, click the **CCM Devicepool Management** button.
- Step 2** Click the **Add** button.
- Step 3** Complete all of the required fields and click the **Add** button.

The device pool is added to the system.

The available fields include:

Field	Description
<i>Device Pool</i>	Enter the name of the device pool. This is a mandatory field.
<i>CCM Group Name</i>	Select the required CCM group name from the drop-down list. This is a mandatory field.

Site Code Management for Buildings

Procedure

Adding Site Codes

To add a site code for a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the building *Name* (active text link) that you would like to add a site code for.
- Step 3** Click the **Site Codes** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required fields. The following fields are available when adding a site code:

Field	Description
Site Code Rules	The rules that apply for new site codes, for example, "Site Code Max 4 digits".
Site Code	The site code being added. This must comply with any rules defined in the above field. This is a mandatory field.
Last Site Code in range	This is an optional field and is used to define the last site code in a range of site codes.

- Step 6** Click the **Add** button. The site code is added to the system.

Procedure

Deleting a Site Code

To delete a site code:

- Step 1** From the Building Management screen, click the **Site Codes** button.
- Step 2** Click the **Delete** button adjacent to the site code that you would like to delete.
-

The site code is removed from the system.

Managing Building Voicemail Services

Voicemail services enable the recording and storage of voice messages for end-users when they are either busy or away from their phones.

Note

- For Voicemail accounts to be created for end-users, the services have to be created as a resource by the Provider administrator for each Customer and then created as a Service in each Location.
 - Voicemail resources at the Provider level require a Site Code to be created before you can add the Voicemail Resource. The Site Code must be created within the Customer; hence the Voicemail resource is tied to that Customer. The Voicemail Service in effect becomes a special Location within the Customer and E164 numbers can then be moved into the Voicemail Resource.
 - Voicemail resource must be allocated a Pilot Number(s). The pilot number is required when a Location Voicemail Service is created to identify it within the Voicemail system. The Pilot Number is used by Users to call the Voicemail system to retrieve messages against their account (i.e. Line) number.
-

From the *Manage Building Voicemail Services* screen, you can view, modify and add voicemail services.

Add a Voicemail Service

Procedure

To configure a voicemail service for a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the building *Name* (active text link) that you would like to add a voicemail service for.
- Step 3** Click the **Voicemail** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required fields. The following fields are available when adding a voicemail service:

Field	Description	Remarks
Name	The name of the Voicemail Service being added.	This is a mandatory field. The name must be unique.
Description	A short description of the Voicemail Service being added.	-
Country	The Country within which the Voicemail Service operates.	This is a mandatory field.

Field	Description	Remarks
Site code	The site code where the Voicemail service is operating.	This is a mandatory field. The Site Code can be a maximum of four (4) digits.
Voicemail Server Hardware Group	The hardware group that houses the voicemail server that the service utilizes.	This is a mandatory field. The Voicemail server must be added to the hardware group before the Voicemail service can be added.
Extension Length	Select the required Extension length from the drop-down list.	This is a mandatory field.
Voicemail PSTN Dial Prefix	The PSTN prefix that is used to access the Voicemail service.	This is a mandatory field.
Voicemail Server	Select the required voicemails server from the drop-down list.	This is a mandatory field. The available list of servers is influenced by the hardware group selected.

Step 6 Click the **Add** button. The voicemail service is added to the system.

Modifying a Voicemail Service

Procedure

To modify a voicemail service:

- Step 1** From the *Building Management* screen, click the **Voicemail** button.
- Step 2** Select the Voicemail Service *Name* (active text link) that you would like to modify.
- Step 3** Click the button appropriate to your requirements.

Note

The fields displayed on the *Manage Building Voicemail Service* screen cannot be modified and are displayed for information purposes only.

The following functions are available from this page:

Button	Description
Internal Number Management	This screen enables the management of extensions within a building. The page lists all available internal numbers, the <i>Allow</i> or <i>Prevent</i> active text links enables administrators to control the use of these numbers within the building.
PSTN Published Number	This screen enables you to specify and manage a PSTN published number for the building. From this page you are able to add a PSTN number, modify the number and delete the number.
PSTN Number Management	This screen enables you to manage your external number (E164) usage. You are able to manage range associations and manage the DDI and extension numbers.
View Pilot Numbers	This screen enables you to manage the pilot numbers related to the buildings voicemail service.

Button	Description
Voicemail Profile Management	This screen enables you to manage your voicemail profiles. From here you are able to select the available voicemail profiles.

Deleting a Voicemail Service

Procedure

To delete a voicemail service:

- Step 1** From the Building Management screen, click the **Voicemail** button.
 - Step 2** Select the Voicemail Service *Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button.
-

The voicemail service is removed from the system.

Voicemail Pilot Number Management

A pilot number is the address or location of a group, or feature, within a PBX or IP-PBX and is generally defined as a blank extension number or an extension from a that does not have a person or telephone associated with it. When using a voicemail service, each service must be associated to a pilot number. The pilot number is used to locate the service and in turn to locate the telephone extension number on which the incoming call was received. Without a defined pilot number, the PBX or IP-PBX cannot locate where the incoming call was received.

Note

Before assigning a pilot number, please ensure that there are available pilot numbers within your system.

Procedure

Assigning a Pilot Number

To add a pilot number:

- Step 1** Browse to *General Administration > Buildings*.
 - Step 2** Click the **Voicemail** button.
 - Step 3** Select the Voicemail service *Name* (active text link) that you would like to modify.
 - Step 4** Click the **Pilot Number** button.
 - Step 5** Click the **Add** button.
 - Step 6** Complete all of the required fields and click the **Add** button.
-

The Pilot Number is added to the system.

The following fields are available when assigning a pilot number:

Field	Description
Service Name	This is the Voicemail service name and cannot be configured, here, by the user.
Description	A short description of the pilot number being assigned

Field	Description
Select Pilot Number	Select the required pilot number from the drop-down list. This is a mandatory field.
Name	Enter a name for pilot number. This is a mandatory field.

Procedure

Modifying a Pilot Number

To modify a pilot number:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Click the **Voicemail** button.
- Step 3** Select the Voicemail service *Name* (active text link) that you would like to modify.
- Step 4** Click the **Pilot Number** button.
- Step 5** Select the *Pilot Number* (active text link) that you would like to modify.
- Step 6** Modify the required fields and click the **Modify** button.

The Pilot Number is modified within the system.

Procedure

Deleting a Pilot Number

To delete a pilot number:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Click the **Voicemail** button.
- Step 3** Select the Voicemail service *Name* (active text link) that you would like to modify.
- Step 4** Click the **Pilot Number** button.
- Step 5** Click the **Delete** button adjacent to the *Pilot Number* that you would like to delete.

After confirming the deletion operation, the pilot number is deleted from the service.

Selecting the Required Voicemail Service Profile

Procedure

To select the required voicemail service profile for a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the building *Name* (active text link) that you would like to modify the voicemail service for.
- Step 3** Click the **Voicemail** button.
- Step 4** Select the Voicemail service *Name* (active text link) that you would like to modify.
- Step 5** Click the **Voicemail Template Mgt** button.
- Step 6** Select the required voicemail service type checkboxes, and then click the **Update** button. The voicemail profile is updated.

Manage Building Auto Attendant Services

Note

The pilot numbers for the auto attendant and voicemail service numbers both need E164 numbers allocated to them.

[Adding an Auto Attendant Service on page 733](#)

Procedure

Modifying an Auto Attendant Service

The actual values within the Auto Attendant service cannot be edited, only the related pilot numbers can be modified. Follow these steps to modify pilot numbers related to an Auto Attendant service:

- Step 1** From the Building Management screen, click the **Auto Attendant** button.
 - Step 2** Select the Auto Attendant service *Name* (active text link) that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button.
-

The feature group is modified within the system.

Procedure

Deleting an Auto Attendant Service

To delete an Auto Attendant service:

- Step 1** From the Building Management screen, click the **Auto Attendant** button.
 - Step 2** Select the Auto Attendant service *Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button.
-

The Auto Attendant service is removed from the system.

Allocating E164 Numbers to the Voicemail and Auto Attendant Services

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps.

The pilot numbers for the auto attendant and voicemail service numbers both need E164 numbers allocated to them.

Procedure

To allocate the required E164 numbers:

- Step 1** Browse to *Resources > E164 Inventory*.
- Step 2** Select the relevant country from the drop-down list then click the **Next >>** button.

- Step 3** If you need to add an area code for the E164 number, click the **Area Code Mgt** button, alternatively, skip to step 4.
- a** Click the **Add** button.
 - b** Complete the required fields then click the **Add** button.
 - c** Return to the E164 Number page by repeating steps 1 and 2.
- Step 4** Click the **Add Number Range** button.
- Step 5** Complete the required fields then click the **Add** button.
- Step 6** Return to the E164 Number page by repeating steps 1 and 2.
- Step 7** Click the **Move Number Range** button.
- Step 8** Complete the required fields and click the **Add** button.

Note

When asked to select the location, specify the service created in the previous steps, for example, select: *FRTest-buildingVoicemail-test1*

Adding an Auto Attendant Service

Procedure

To add an auto attendant service:

- Step 1** Browse to **General Administration > Buildings**.
- Step 2** Select the building *Name* (active text link) that you would like to add an auto attendant service to.
- Step 3** Click the **Auto Attendant** button.
- Step 4** Click the **Add** button.
- Step 5** Complete all of the required fields. The following fields are available when adding an auto attendant service:
- | Field | Description |
|---------------------------|--|
| Name | Specify the name for the auto attendant service. This is a mandatory field. |
| Description | A description of the auto attendant service. |
| Country | Select the relevant country from the drop-down list. This is a mandatory field. |
| IVR Server Hardware Group | Select the required IVR Server Hardware Group from the drop-down list. This is a mandatory field. |
| Extension Length | Select the required extension length from the drop-down list. This is a mandatory field. |
| IVR Server | Select the IVR server that you would like to use for this service from the drop-down list. This list is influenced by the hardware group selected on the previous page. This is a mandatory field. |
- Step 6** Click the **Add** button.
- Step 7** Select the required *IVR server* then click the **Add** button. The auto attendant service is added to the system.
-

Building Auto Attendant Pilot Number Management

A pilot number is the address or location of a group, or feature, within a PBX or IP-PBX and is generally defined as a blank extension number or an extension that does not have a person or telephone associated with it. When using an Auto Attendant service, each service must be associated to a pilot number. The pilot number is used to locate the service and in turn to locate the telephone extension number on which the incoming call was received. Without a defined pilot number, the PBX or IP-PBX cannot locate where the incoming call was received.

Note

Before attempting to modify pilot numbers, please ensure that there are available pilot numbers within your system.

Procedure

Modifying a Pilot Number

To modify a pilot number:

- Step 1** Click the **Auto Attendant** button.
 - Step 2** Select the Auto Attendant *Name* (active text link) that you would like to modify a pilot number for.
 - Step 3** Click the **View Pilot Numbers** button.
 - Step 4** Select the *Pilot Number* (active text link) that you would like to modify.
 - Step 5** Modify the required fields and click the **Modify** button.
-

The pilot number is modified within the system.

Procedure

Deleting a Pilot Number

To delete a pilot number:

- Step 1** Select the **Auto Attendant** button.
 - Step 2** Select the Auto Attendant *Name* (active text link) that you would like to delete a pilot number from.
 - Step 3** Click the **View Pilot Numbers** button.
 - Step 4** Select the Pilot Number *Name* (active text link) that you would like to delete.
 - Step 5** Click the **Delete** button.
-

After confirming the deletion operation, the pilot number is deleted from the service.

Feature Group Management

All telephony and value added features managed by the system are defined as Features. Any single version of the system supports a defined set of features. These features are then Grouped together to form a Feature Group, which is then associated with a phone or user and defines the set of features the person or phones has access to.

From the *Manage Building Feature Groups* screen, you can view, modify and add feature groups.

[Adding Feature Groups on page 735](#)

Bulk Updating Feature Groups .

Refer to *Bulk Updating Feature Groups* in [Feature Group Management on page 500](#).

Procedure

Modifying a Feature Group

To modify a Feature Group:

- Step 1** From the Building Management screen, click the **Feature Groups** button.
 - Step 2** Select the Feature Group *Name* (active text link) that you would like to modify.
 - Step 3** Modify the required fields and click the **Modify** button. For a description of the available fields refer to [Features Available when Adding or Modifying a Feature Group on page 505](#).
-

The feature group is modified within the system.

Procedure

Deleting a Feature Group

To delete a Feature Group:

- Step 1** From the Building Management screen, click the **Feature Groups** button.
 - Step 2** Select the Feature group *Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button.
-

The feature group is removed from the system.

Procedure

Copying a Feature Group

To copy a Feature Group:

- Step 1** From the Building Management screen, click the **Feature Groups** button.
 - Step 2** Click the **Copy** button.
 - Step 3** Type in the new feature group name in the text field adjacent to the *Feature Group* that you would like to copy.
 - Step 4** Click the **Copy** button adjacent to the Feature Group that you would like to copy.
-

The feature group is created within the system.

Adding Feature Groups

Note

For more information on feature groups, please see the *Feature Groups* section.

Procedure

To add a feature group to a building:

- Step 1** Browse to *General Administration > Buildings*.
 - Step 2** Select the building *Name* (active text link) that you would like to manage.
 - Step 3** Click the **Feature Groups** button.
 - Step 4** Click the **Add** button.
 - Step 5** Complete the required fields. For a description of the available fields refer to [Features Available when Adding or Modifying a Feature Group on page 505](#).
 - Step 6** Click the **Add** button. The feature group is added to the building.
-

Customer Building Management

Procedure

Add a new Location for an Existing Customer

To add a new location for an existing customer:

- Step 1** Browse to *General Administration > Buildings*.
 - Step 2** Select the building *Name* (active text link) that you would like to add the customer to.
 - Step 3** Click the **Customer** button.
 - Step 4** Click the **Add** button.
 - Step 5** Click the **Add** button adjacent to add a new Location for an existing Customer.
 - Step 6** Complete the required fields then click the **Add** button. For available fields, see: [Adding a Customer to a Building on page 736](#)The location is added to the system.
-

Procedure

Deleting a customer

To delete a customer:

- Step 1** From the *Building Management* screen, select the **Customers** button.
 - Step 2** Select the Customer *Name* (active text link) that you would like to delete.
 - Step 3** Click the **Delete** button.
-

The customer is removed from the system.

Adding a Customer to a Building

Procedure

To add a customer to a building:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the building *Name* (active text link) where you would like to add the customer.
- Step 3** Click the **Customer** button.
- Step 4** Click the **Add** button.

Step 5 Click the **Add** button adjacent to add a new customer.

Step 6 Complete the required fields. The following fields are available when adding a customer:

Field	Description	Remarks
Customer Name	The name of the Customer being added.	This is a mandatory field. The name must be unique and
Extended Customer Name	Used for expanding on the customer's name.	This is an optional field.
Division Name	The name of the division where the customer is present.	-
Extended Division Name	Used for expanding on the division name.	This is an optional field.
Location Name	The name of the Location where the customer is present.	This is a mandatory field.
Localized Location Name	The name of the Location in relation to the customer and building.	This is an optional field. Can be used to present a customer with a more logical location name.
Extended Location Name	Used for expanding on the location name.	This is an optional field.
Address	Address field of the customer.	-
City	City where the customer is located.	-
State	State where the customer is located.	-
Post/ZIP Code	Post/ZIP Code where the customer is located.	-
Country	Country where the customer is located.	-
TimeZone	The time zone relevant to the customer.	This is a mandatory field. Select the time zone that is relevant to the customer from the drop-down list.
Contact Name	Contact Name of the person responsible for the customer.	-
Contact Fax Number	Fax number for the person responsible for the customer.	-
Telephone Number	Telephone number for the person responsible for the customer.	-
Contact Email	Email address for the person responsible for the customer.	-
Customer account number to use in external accounting system	The relevant account number to use for any billing transactions related to the customer.	-
Location account number to use in external accounting system	The relevant location account number to use for any billing transactions related to the customer.	-
Directory IP Address	The IP address for the customer's corporate directory.	-
Site Code	The location site code.	-

Field	Description	Remarks
Extension number length	The length of extension numbers.	This is a mandatory field.
National Code	The national code.	This is a mandatory field.
Select Managed IP Subnet to assign to Location	<p>The managed IP subnet assigned to the location. Select from the drop-down list</p> <p>Note</p> <p>The drop-down list only displays all unused subnets, all used subnets shared at this cluster, and only subnets with the same IP Edge device as this building if one has been chosen.</p>	This is a mandatory field.
Voicemail Service	The voicemail service.	Select the relevant voicemail service.
Auto Attendant service	The auto attendant service.	Select the relevant auto attendant service.
Default branding of User Interface	The default branding for the user interface.	Select the default branding for the user interface.
Default GUI branding	The default GUI branding.	Select the default GUI branding.
Enter number of lines required	The required number of lines for each line type.	Enter the required number of lines for each line type.
Enter the number of phones required	The required number of phones for each phone type.	Enter the required number of phones for each phone type.
Enter subscriber numbers	The required number of subscribers for each service.	Enter the required number of subscribers for each service.
Allowed extension ranges	The ranges allocated to phones.	Enter the ranges allocated to phones.
Voicemail service name	The voicemail service name.	Select the relevant voicemail service name.
Pilot Number	The pilot number.	Select the relevant pilot number.
PSTN Number	The PSTN number.	Select the relevant PSTN number.
Location Voicemail service name	The location voicemail service name.	Select the relevant voicemail service name.
Auto Attendant service name	The auto attendant service name.	Select the relevant auto attendant service name.
Pilot Number	The pilot number.	Select the relevant pilot number.
PSTN Number	The PSTN number.	Select the relevant PSTN number.
Location Auto Attendant Service Name	The location auto attendant service name.	Select the relevant Location Auto Attendant service name.

Step 7 Click the **Add** button. The customer is added to the system.

Note

When you create customers by using this menu, it triggers a meta-transaction that automatically creates division and location along with the customers. You

can also add Voicemail and Auto Attendant service pilot numbers if Voicemail and Auto Attendant services are already created in the Building.

Manage Building Preferences

Building preferences and settings are covered as well as the allocation of a phone to a building and the assignment of numbers and management of users and phones.

Managing a Building Preferences and Settings

The *Manage Building Preferences* screen enables you to manage the preferences available to customers in the building. The three options include:

- Preferences for this building
- Default preferences for new Customers in this building
- Default preferences for new Locations in this building

Refer to [Available Preferences and Settings on page 934](#) for details.

Managing a Building's Details

Procedure

To modify a building's details:

- Step 1** Browse to *General Administration > Buildings*.
 - Step 2** Select the building *Name* (active text link) that you would like to modify.
 - Step 3** Modify the required details and click the **Modify** button. The building details are updated.
-

Allocating an E164 Number Inventory to a Building (Location)

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps - see [Specifying the Area Code on page 574](#).

Procedure

To allocate E164 numbers to a location:

- Step 1** Browse to *Resources > E164 Inventory*.
 - Step 2** Select the required country that you would like to add the number range to from the drop-down list, and then click the **Next >>** button.
 - Step 3** Select relevant National Area Code from the drop-down list, and then click the **Next >>** button.
 - Step 4** Click the **Move Number Range** button.
 - Step 5** Specify the following details: location, start of number range and end of number range.
 - Step 6** Click the **Move** button. The numbers are moved to the specified location.
-

Allocating a Phone to a Building (Location)

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps.

Procedure

To allocate a phone to a location:

- Step 1** Browse to *Resources > Phone Inventory*.
 - Step 2** Select the *Device Name* (active text link) of the phone that you would like to move.
 - Step 3** Select the required Move target location from the drop-down list.
 - Step 4** Click the **Next >>** button.
 - Step 5** Select the required subnet (if applicable) from the drop-down list, and then click the **Add Phone** button.
-

Building Voicemail Service - E164 Number Management

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps.

Procedure

To add a PSTN published number:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the location *Name* (active text link) where you would like to add the PSTN published number.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **PSTN Published Number** button.
 - Step 5** Specify the published PSTN number then click the **Add** button. The PSTN published number is added to the system.
-

Procedure

Deleting a Published PSTN Number

To delete a Published PSTN Number:

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Select the *Voicemail service* (active text link) that you would like to delete the Published PSTN Number from.
- Step 3** Click the **Published PSTN Number** button.

- Step 4** Click the **Delete** button.

The Published PSTN Number is deleted from the Voicemail Service.

Procedure

Modifying a Published PSTN Number

To modify a Published PSTN Number:

- Step 1** Browse to *Resources > Voicemail Services*.
- Step 2** Select the *Voicemail service* (active text link) that you would like to modify the Published PSTN Number for.
- Step 3** Click the **Published PSTN Number** button.
- Step 4** Modify the Published PSTN Number then click the **Modify** button.

The Published PSTN Number is modified.

Note

It is important to ensure that the correct format is used for the Published PSTN Number, otherwise, certain calls may fail. The required format is dependent on the configuration of your dial plan, please refer to the *Deployment Guide* for further information.

PSTN to Extn Range Mapping

Procedure

Associating a Range of PSTN numbers

To associate PSTN numbers with a voicemail service:

- Step 1** Browse to *General Administration > Buildings*.
- Step 2** Select the required building *Name* (active text link).
- Step 3** Click the **Voicemail** button.
- Step 4** Select the required voicemail service *Name* (active text link).
- Step 5** Click the **PSTN Number Mgt** button.
- Step 6** Click the **Associate Range** button.
- Step 7** Complete all of the required fields and click the **Add** button.

The PSTN range is associated with the voicemail service.

Procedure

Disassociating a Range of PSTN numbers

To disassociate PSTN Numbers with a voicemail service:

- Step 1** Browse to *General Administration > Buildings*.

- Step 2** Select the required building *Name* (active text link).
 - Step 3** Click the **Voicemail** button.
 - Step 4** Select the required voicemail service *Name* (active text link).
 - Step 5** Click the **PSTN Number Mgt** button.
 - Step 6** Click the **Disassociate Range** button.
 - Step 7** Complete all of the required fields and click the **Add** button.
-

The PSTN range is disassociated from the voicemail service.

Adding an Emergency Published Number

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps.

Procedure

To add an Emergency Published Number:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the location *Name* (active text link) where you would like to add the emergency public number.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Emergency Number** button.
 - Step 5** Specify the required number then click the **Add** button. The emergency published number is added to the system.
-

Assigning an E164 Number Range to Internal Numbers

Note

Depending on the administrator's hierarchy, a more privileged administrator may need to carry out these steps.

Procedure

To assign a range of E164 numbers to internal numbers:

- Step 1** Browse to **Location Administration > External Numbers**.
 - Step 2** Click the **Associate Range** button.
 - Step 3** Select the required national code.
 - Step 4** Click the **Next >>** button.
 - Step 5** Complete the required fields then click the **Submit** button. The E164 number range is assigned to the internal numbers.
-

Note

If the *AssociateFNNinRanges* preference is enabled, you must specify your required range size during the above process.

Managing Users and Phones

Even though they are part of a building, users and their phones are managed in the same manner as phones and users within a normal location. Refer to the *Location Administration* section for information on managing users, their phones and mobility profiles.

Operations Tools

Operation Tools allow for the automation of multi-step processes, such as de-registering all phones in a location. The following operation tools are available:

Operation Tool	Description	Remarks
Set Dial Plan Codecs	Sets the system level codecs for Intra-Location Max Audio Bit Rate and the Inter-Location Max Audio Bit Rate.	Use the drop-down lists to select the <i>Intra-Location Max Audio Bit Rate</i> and the <i>Inter-Location Max Audio Bit Rate</i> , select the <i>Customer/Building Codec Configurable?</i> checkbox if you would like customers/buildings/locations to be able to select their own codecs, then click the Submit button.
Destroy a building (All locations in it)	Destroys a building and all locations in it	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>



CHAPTER 8

Location Administration

- Managing locations **745**
 - Location Administration - Quick Reference **746**
 - Hierarchy Levels **746**
 - Finding a location **747**
 - Deleting a Location **748**
 - Adding a location **749**
 - Managing a Location **757**
 - Location Main Page **758**
- The PBR Process Using Bulk Loaders **789**
- The PBR Process Using the system GUI **795**
- Phone Management **803**
 - Managing the Phone **806**
 - Manage Lines **810**
 - Manage Speed Dials **814**
 - Busy Lamp Fields **815**
 - Manage Service URL **817**
 - Login User **818**
 - Phone Alerting Names **818**
 - Contact Center Agent Lines **819**
 - Replace a Phone **819**
 - Unregistering / Deleting a Phone **820**
- Location Administration Tools **821**
- Unmanaged Locations **822**
 - Adding an Unmanaged PBX **822**
 - Adding a Hardware Group for Unmanaged Locations **822**
 - Adding an Unmanaged Location **823**
 - Location Administration for Unmanaged Locations **823**
 - Allocated Connectivity for the Location **823**
- Resource Management **823**
 - Managing Available Internal Numbers **824**
 - External numbers **826**

Phone Inventory	830
Managing Users	839
Find a User	839
Delete a User	841
Add an End User	842
Manage an End User	846
Reset User's Password	850
Unlocking a locked User account	851
Reset User's Phone PIN	851
Associate/Unassociate (or Delete) Device with/from User	852
Extension Mobility Profiles	854
Manage Voicemail Accounts	867
Create Voicemail Account	870
WebEx Conferencing	873
UC Central	874
Administration Users	876
Managing Numbers	884
Telephony Management	884
Number Group Management	897
Hunt Group Management	901
Pickup Groups	905
Presence Monitoring	910
Location License Management	911
Self Care Skinning	914
Theme Management	914

Managing locations

A Location is the location/site within an organization/company that actually receives the telephony service. During the creation of each Location, the following must either be defined or allocated as required:

- The maximum number and type of Lines, Phones and Services. These limits can later be increased/decreased to reflect the expansion/contraction of a Location.
- An IP Subnet is defined. Additional Subnets may be defined later.
- The PSTN National *Area Code* required by the Location is defined.
- A *Published Number* is defined. This is the number typically used by external callers to reach the Location.
- Based on the earlier selection, Internal Extension numbers and PSTN lines are allocated to the Location.

From the *Location Management screen*, administrators are able to add, modify, view and delete Locations. For further information, please view [Adding a location on page 749](#) and [Location Administration - Quick Reference on page 746](#).

After having created the location and defined the number of phones required etc., the next step is to decide on the method by which phones are to be deployed and registered. The two options are:

- **Administrator controlled phone move:** Using this option, an administrator selects the phones, by its Device name, to be moved into to a specific Location. Once a phone has been moved into a specific location, it will only ever connect to that to the IP Telephony network from that location. If the phone is connected in the correct Location, the system will ensure it is provided with an appropriate IP address and registered on the correct IPPBX. At this stage the phone may be provisioned as required i.e. Have the appropriate Lines attached and features activated.
- **Automatic phone move:** Using this option, the device name of the phones being deployed within a Location do not have to be defined in advance. The phones can be shipped to the required Location and connected. The system then detects which Location they are connecting from and automatically assigns the phone to the correct Location, leaving the phone ready to be provisioned.

Location Administration - Quick Reference

How do I?	Steps to take
Register a phone	Browse to Location Administration > UserName > Associate Phone > Select the Device name of the phone to register > Feature Group > Select Softkey Template and Line Number .
Add an Extension Mobility Profile for a User	Choose General Administration > Users > UserName > Extension Mobility Profile > Select correct numbers for User > Add
Add Speed Dials for a User	Choose Self Care Menu of relevant User > Mobility > SpeedDials tab > Enter details > Add
Manage Internal Numbers	Choose Location Administration > Internal Numbers > Internal Number Range Mgt tab> Select Enable or Disable
Add Number Groups to Locations	Choose Location Administration > Number Groups > Enter required behavior options, Distribution Method, Ring no answer options and Line Number > Add
Add a Number to a Number Group	Choose Location Administration > Select Number Groups > Select the Number Group > Add Number > Select the Number > Add
Manage/Modify a Hunt Group	Choose Location Administration > Hunt Groups > Select the required Hunt Group > Modify as required > Modify
Adding Numbers to a Pickup Group	Choose Location Administration > Select Pickup Groups > Select Add Number > Select the required Number > Add
Associate Pickup Groups	Choose Location Administration > Select Pickup Groups > Select the name of the Pickup Group > Select Associate > Select the Pickup Group to Associate with the above group > Select Associate
Add a Voicemail account for a User	Select General Administration > Users > UserName > Voicemail > Personal Voicemail Enter a password for the Voicemail account and select the Add button

Hierarchy Levels

The following hierarchical levels are supported in the system. These are used for general management tasks as well as for managing the use of resources (from the highest to the lowest user level):

- Provider
- Reseller

- Building
- Customer
- Division
- Location
- User (End-user)

There are different types of resources available:

- Physical and Network Resources (e.g. Phones, IP Addresses)
- Services (e.g. Voicemail, Conference)
- General / Supporting data (e.g. Site codes)

The following table provides a high level guideline of resource management and the hierarchy level from which you can manage the resource:

Resource	Type	Managed at level:	Used at level
<i>E164 Numbers (DDIs / DIDIs / FNN)</i>	Physical	1 and 5	5
<i>Billing Codes</i>	General	1 to 7	2 to 7
<i>Managed IP Subnets</i>	Physical	1 and 3	5
<i>Site Codes</i>	General	3	5
<i>Voicemail</i>	Service	3 and 5	7
<i>Auto Attendant</i>	Service	3 and 5	4
<i>Console</i>	Service	3 and 5	5 and 7
<i>Media</i>	Service	3 and 5	5 and 7
<i>Phones</i>	Physical	1 to 4	5
<i>Contact Center</i>	Service		
<i>Analog lines</i>	Physical		5
<i>MoH</i>	Service	5	7
<i>Internal Numbers (extensions)</i>	Physical	5	7
<i>External Numbers</i>	Physical	5	7

Finding a location

There are several ways to find a specific location:

- Via *General Administration > Locations* menu. Navigate through the hierarchy, for example: Provider, Reseller, Customer and Division, to find the list of locations at the selected level.
- Via the *Quick Search* active text link at the top right of the page - see: [Search For on page 534](#).

Procedure

Location search from General Administration

Follow these steps:

- Step 1** Select *Locations* from the *General Administration* menu. The resulting screen shows the first 50 location names (by default) in that division.

Note

To manage a specific location, select the active text link of the *Location Name*.

Step 2

To find a specific location, select the search criteria from the *Search by* pull-down selection list, and type as many characters as you know in the field provided, and then click the **Search** button. The following search criteria are available:

- *Location Name*: All or part of the location name (e.g. "lo" = all locations that have the letters "lo" in their location name)
- *City Name*: The city last name or part of it (e.g. "smi" = all locations that have the letters "smi" in their city name)
- *Site Code*: The numeric code assigned to the location, or part of it.

Note

The search string is not case-sensitive.

The following information is shown per location in the Location list

Field	Description	Remarks
Location Name	Active text link	When used (selected) this opens a screen with the location details allowing you to manage this specific location.
Address	The address details of the location	-
Site Code	The allocated site code for the location.	
Location Type	Type of location, for example, Standard Location, Linked Location Parent or Unmanaged Location.	

See also: [Managing a Location on page 757](#).

Deleting a Location

This deletes the existing locations details from the system. The system de-provisions the location in the platform and clears the location from its database.

Note

You cannot delete a Location while there are Phones and Users located within the Location. Phones and Users must be deleted from the Location before the Location can be deleted.

Note

When deleting a location, and the delete process fails after all the device pools have been removed, a new 'typical' device pool is created for the location.

Procedure

To delete a Location:

- Step 1** Browse to *General Administration > Locations*.
- Alternatively,**
- Browse to the required location via the *Location Administration* Menu and skip to Step 3.
- Step 2** Select the *Location Name* (active text link) that you want to delete.
- Step 3** Click the **Delete** button.

The location is deleted from the system.

Adding a location

When adding a new location, first confirm that the following steps have been completed by your provider:

- A parent customer and division exist.
- The new location has cabling installed within the building and individual offices are connected.
- The line-powered switch has been installed on-site at the new location and connected to the service provider network.

Obtain the following information from the service provider before adding a location:

- Hardware Group for the location: for example, QT-P1-PGW1-C1-CP
- Internal Site code for the location: for example, 7101
- PSTN Area code for the location: for example, 4
- Customer location standards: Internal ext length, internal ext range
- If Applicable
 - Primary location Number (i.e. main number): for example, 86644000
 - Emergency Number (for callback by emergency services): for example, 86644001
 - Information regarding the applicable voicemail service for the location
 - Information regarding location preferences which require setting on or changing for a specific value
 - Details of the subnet(s) to allocate to the location.

Note the following when adding locations:

- A location administrator cannot add a new location. Only customer administrators or higher (including customer administrators) are authorized to add locations.
- You must add a location from the *Location Management* page.

Additional operational considerations

To use devices in the location, you need to go through additional steps adding E164 numbers, phones, users to the location, associating the relevant items and registering the phones. All of this can be done only after the location has been successfully created.

Therefore, before you create your location, you may want to check that you have the following information as well:

- The E164 telephone numbers have been identified for allocation to the location.

- Phones for the location have been identified at the Provider/Reseller level (list of phone Device Names), and are available to be allocated to the new location (for example, 12.34.56.78.AB.90).
- Required information for location users has been identified and user standards are agreed.

Procedure

To add a location via the general administration menu (*General Administration > Locations*):

The *Location Administration* screen displays the existing locations for the current division.

To add a new location:

Step 1 Browse to *General Administration > Locations*.

Step 2 Click the **Add** button.

Note

Depending on the configuration of your system, available fields may vary.

Step 3 Complete the required fields.

Field	Description	Remarks
Details:		
Location Name	The name of the location.	This is a mandatory field. Must be unique across platform.
Localized Location Name	A more detailed description of the location.	This is an optional field.
Extended Location Name	A more detailed description of the location.	This is an optional field.
External Location ID	This field enables an external system to map a Location ID to an external Location ID. For example, if the Location ID is Location_123 but an organizations billing system uses a location reference of London_South_Site-123, the External Location ID field can be specified as London_South_Site-123.	This is an optional field. This field is limited to a maximum of 100 characters and must be unique within the Provider/Reseller/Customer realm.
Department	Use this field to enter a cost center for the location.	This is an optional field. For example, Sales, Finance etc.
Department code	Cost center code.	This is an optional field.
Address 1, 2, 3	Details of the locations address.	These are optional fields.
City	The City in which the location is situated.	This is an optional field.
State	The State in which the location is situated.	This is an optional field.
Country	The Country in which the location is situated.	This is a mandatory field. Select from the drop-down list, default = the country of the division to which the location is being added.

Field	Description	Remarks
TimeZone	The time zone in which the location is situated.	<p>This is a mandatory field. The time zone that is selected here is used by the typical default device pool if it is selected as part of the configuration - see: Add Location - Page 3 on page 753 and Adding a Device Pool Template on page 559.</p> <p>This time zone is also shown when adding pilot numbers for Voicemail and Conference Center services - see: Voicemail Pilot Number Management on page 730 and Conference Service Pilot Numbers on-page 631.</p> <p>Note</p> <p>The time zone option selected from the drop-down list must correspond with an existing date/time group in the associated Unified CM, otherwise the add location transaction will fail.</p>
Post/Zip Code	The relevant post/zip code for the selected location.	This is an optional field.
Contact Name	Contact details of the location administrator.	This is an optional field.
Override Language	Select from the drop-down list a language to apply as the location's default language.	The 'default' option will keep the location's default language as the language that was set at the associated customer. Note: This field is only available if the Enable Admin GUI Translation field has been set for the Customer.
Contact telephone number	Contact details of the location administrator.	This is an optional field.
Contact Fax Number	Contact details of the location administrator.	This is an optional field.
Contact Email	Contact details of the location administrator.	This is an optional field.
Account number to use in external accounting system	Specify the account number to use if an external accounting system is being used.	This is an optional field.
Security profile	Select the required security profile from the drop-down list.	This is an optional field.
Directory Partition	Select the partition available to the location if available - see: Corporate Directory Partitions on page 638 .	This is an optional field.

Field	Description	Remarks
Location Type	Select the required location type from the drop-down list, for example, Shared Location.	This is an optional field.

Step 4 Click the **Next** button.

Add Location - Page 2

Procedure

Step 1 Enter the relevant Location hardware details. The following table describes the fields available on the second Add Location page:

Field	Description	Remarks
Location Name	The name of the location as entered on the first screen.	Read only field.
Hardware Group	Defines a set of hardware devices e.g. PBXs, Gateways etc on the network which will be used by the location.	This is a mandatory field. Select from the drop-down list.
PBX Template	The PBX Dial Plan template for this location.	This is a mandatory field. Select from the drop-down list.
Enhanced Emergency Support	When this option is selected, functionality such as emergency number callback is activated.	This is an optional field.
Single Number Reach Support	Select this option if the location requires Single Number Reach support.	This is an optional field.
Dial Plan		
Site code	The short-code dial prefix before internal direct dial numbers. This will enable internal calls between sites to be routed directly over the internal network.	Select a specific site code from the drop-down list or allow the system to allocate the site code (Auto Allocated). The Site Codes are unique at customer level and will have been set up by the Customer Administrator.
Dial to get outside line	Prefix used to enable outside dialling.	Select from the drop-down list.
Select extension number length	Maximum numbers allowed for internal extensions.	Select from the drop-down list. Minimum and maximum allowed length are determined by the number rules set by the Service Provider. Please obtain this information from your customer administrator.
Default Area Code	The location area code.	Select from the drop-down list, aka national code.
Local Dialling	Select the required local dialling length, either 7 or 10 digits.	This is a mandatory field.

Field	Description	Remarks
Subnets		
Select Managed IP Subnet to assign to Location	The logical group of IP Addresses, allocated for use at this location.	<p>Select from the drop-down list.</p> <p>An IP Subnet is a logical group of IP Addresses, normally based on the private address range within a Provider or Customer. A unique IP address range (or Subnet) is assigned to each Location. Subnets can be various sizes, depending on the size of the Location. Obtain the information regarding the subnet allocated for your location from your Service Provider.</p>
Media Services		
Name	The media service.	<p>Select from the drop-down list.</p> <p>Media services are created by the Provider for each Customer and then managed by the Customer Administrator within each Location. Although not mandatory, we recommend that you link the location to a media service at the point of creation to avoid any possible issues later.</p>
GUI Branding:		
Default Branding of User Interface	The branding theme (colors, fonts, items look & feel etc) to be presented to the user when it will log into the system.	<p>Select from the drop-down list.</p> <p>The themes (branding) are defined by the Provider administrator. The applicable themes should be enabled for each level in the system hierarchy. This is a mandatory field.</p>
Default GUI Branding	Determine the default brand.	Select the checkbox to apply the required default GUI theme for this location.

Step 2 Click the **Next** button.

Add Location - Page 3

Procedure

Step 1 Enter the Location IPPBX elements (bandwidth details), line, services and phone type details. The following table lists and describes the fields available on the third Add Location page:

Field	Description	Remarks
Details:		
Use Location for Auto-move	Use this location for Automove.	Select the appropriate checkbox.
IPPBX Elements:		

Field	Description	Remarks
Bandwidth Group	The name of the Bandwidth Group.	Select the required bandwidth group if required from the drop-down list. In this scenario the location is sharing the selected bandwidth group with other locations. .
Voice Bandwidth (kbps)	This determines the voice bandwidth for the location.	Enter the required voice bandwidth for the location. Select the <i>Unlimited</i> radio button for an unlimited voice bandwidth, or enter a specific voice bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field).
Video Bandwidth (kbps)	This determines the video bandwidth for the location.	Enter the required video bandwidth for the location. Select the <i>None</i> radio button for no video bandwidth, select the <i>Unlimited</i> radio button for an unlimited video bandwidth or enter a specific video bandwidth value, for example 512 or 1024 kbps, in the available text field (if the location is not sharing a bandwidth group - see above field).
Device Pool:		
Configuration	Add a device pool as part of the Add Location workflow (not applicable to Unmanaged Locations).	<p>Select the <i>Typical</i> or <i>Custom</i> radio button. If <i>Custom</i> is selected, select the required device pool template from the list of templates available at the location (see also custom device pool fields below). These fields are pre-populated with data, depending on the device pool template selected, edit the fields if required.</p> <p>When <i>Typical</i> is selected, the various device pool fields are hidden. When <i>Custom</i> is selected, these fields are visible. Furthermore, when <i>Custom</i> is selected, selecting a specific device pool template affects the available device pool settings as per the template. The user can switch between <i>Typical</i> and <i>Custom</i>, but the settings specified are only used/applied if the user selects <i>Custom</i>. If the user selects <i>Typical</i> no device pool template or any other device pool settings specified are used; In this case all settings are determined as before, during the add location operation.</p>

Field	Description	Remarks
Name	The device pool name.	<p>Edit if required.</p> <p>Note</p> <p>If the <i>EnableUniqueness</i> setting is Enabled in customer preferences, then the LocationID is appended to the device pool name for <i>Custom</i> device pools. For <i>Typical</i> device pools (only available when adding a location) the LocationID is always appended to the device pool name, regardless of the preference setting. If the <i>EnableUniqueness</i> setting is Disabled, and a user attempts to add a device pool using a device pool name that already exists (on another location), then the creation of the device pool fails. Since the <i>EnableUniqueness</i> preference uses the LocationID, a user can not create device pools with the same name in the same location, even if the preference is Enabled.</p>
Description	A brief description of the device pool.	Edit if required.
Device Pool Type	This is always "Location" when adding a location.	An "SRST" type device pool can only be added when adding a device pool via the <i>Location Administration > Telephony</i> menu option.
Default Device Pool	This checkbox determines if this device pool is the default device pool for the Location.	Select or unselect the checkbox as required.
Device Pool Template	The selected device pool template. This selection determines the field entries below.	This is a mandatory field. Select the required device pool template from the drop-down list of device pool templates available at the location. Note that this field is only available when adding a device pool, not when modifying a device pool.
Call Manager Group	Select from the drop-down list.	<p>Determined by the device pool template (when <i>Custom</i> is used).</p> <p>Note</p> <p>If <i>Typical</i> is used, the least loaded Call Manager Group is used as per the original Add Location workflow.</p>

Field	Description	Remarks
Date/Time Group	Select from the drop-down list.	Determined by the device pool template. Note Date/time groups deleted in Unified CM are no longer displayed in this drop-down if the <i>Import/Refresh CCM Items - Date/Time Groups</i> option has been initiated in CUCDM.
Audio Region	Select from the drop-down list.	Determined by the device pool template, modify if required. This specifies the audio region to assign to devices in this device pool, which in turn specifies the voice codec that can be used for calls within a region and between other regions.
Supported Streams	Device pool voice streams supported are not enforced on number of phones associated. Total device pool streams are constrained to the associated Unified CM Group stream count, that is all device pools using a Unified CM Group cannot exceed in total the Group's stream count.	Enter the required value. Default = 0.
Local Route Group	Determined by the device pool template.	-
AAR CSS	Read-only field.	Determined by the device pool template.
AAR Group	Read-only field.	Determined by the device pool template.
Calling Party Transformation CSS	Read-only field.	Determined by the device pool template.
Called Party Transformation CSS	Read-only field.	Determined by the device pool template.
Allowed Extension Ranges:		
Extension Ranges	The extension ranges, for example, 100-199,300-399.	Specify the required extension ranges, for example, 100-199,300-399.
Codecs:		
Intra-Location Max Audio Bit Rate	Select from the drop-down list the Intra-Region Max Audio Bit Rate to be applied to the location.	Note Codecs can only be set at the customer/building/location level, if the associated dial plan makes provision for it.

Field	Description	Remarks
Inter-Location Max Audio Bit Rate	Select from the drop-down list the Inter-Region Max Audio Bit Rate to be applied to the location.	Note Codecs can only be set at the customer/building/location level, if the associated dial plan makes provision for it.

Step 2 Click the **Add** button when complete. The location is added to the system.

See also:

- [Resource Management on page 823.](#)
- [Managing Available Internal Numbers on page 824.](#)
- [External numbers on page 826.](#)
- [Phone Management on page 803.](#)

Managing a Location

Once a location exists in the system, the administrator can manage or add further elements for it.

Location management consists of the following aspects:

- Location Main Page
 - [General Details on page 758](#)
 - [Additional Information on page 761](#)
- Items applicable for the location as a whole and usually set up once for the location.
 - [Manage Subnets on page 762](#)
 - [Location Preferences Management on page 779](#)
 - Various advanced management options are also available for the location by clicking the **Advanced Mgt.** button - refer to [Advanced Location Management on page 765](#) for more information.

Elements such as phones, users etc. which are changing on a regular basis are more dynamic in their nature. The full list of the dynamic elements is defined in the *Location Administration* menu.

Procedure

- Step 1** Find the Location you want to manage using any of the Find Location options and select it by selecting on the *Location Name* active text link.
- Step 2** Update the applicable details and click the **Modify** button. Refer to [Add Location - Page 3 on page 753](#) for field descriptions if required.

See also: [Finding a location on page 747.](#)

See also: [Deleting a Location on page 748.](#)

Location Main Page

General Details

Location general information is available on the following section of the screen.

The information available in this section for review and update is as follows:

Field	Description	Remarks
Location Name	The name of the location	This is a read-only field.
Localized Location Name	A more detailed description of the location	This is an optional field.
Extended Location Name	A more detailed description of the location	This is an optional field.
Site Code	The short-code dial prefix before internal direct dial numbers as was set when location was created.	This is a read-only field.
Department	Use this field to enter a cost center for the location	This is an optional field. For example; Sales, Finance etc
Department code	Cost center code	This is an optional field.
Address 1,2,3	Details of the location address.	These are an optional fields.
City	Details of the city in which the location is situated.	This is an optional field.
State	Details of the state in which the location is situated.	This is an optional field.
Country	Details of the country in which the location is situated.	This is a read-only field.
TimeZone	Note The timezone option selected from the drop-down list must be a valid timezone that exists in the Unified CM. Details of the time zone in which the location is situated.	This is a read-only field.
Post/Zip Code	The post/zip code of the city.	This is an optional field.
Override Language	Select from the drop-down list a language to apply as the location's default language.	The 'default' option keeps the location's default language as the language that was set at the associated customer. Note: This field is only available if the <i>Enable Admin GUI Translation</i> field on the <i>Customer License Management</i> screen has been set for the Customer.
Contact Name	Contact details of the location administrator.	This is an optional field.
Contact telephone number.	Contact details of the location administrator.	This is an optional field.
Contact Fax Number	Contact details of the location administrator.	This is an optional field.

Field	Description	Remarks
Contact Email	Contact details of the location administrator.	This is an optional field.
Account number to use in external accounting system	-	This is an optional field.
Security profile	Select the required security profile from the drop-down list.	This is an optional field.
Directory Partition	Select the partition available to the location if available - see: Corporate Directory Partitions on page 638 .	This is an optional field.
Enhanced Emergency Support	When selected, this option enables functionality such as Emergency number callbacks.	Checkbox, optional field. This option is location specific and availability may depend on the infrastructure available in your specific area.
Single Number Reach Support	Select this checkbox if you would like to activate Single number reach for a location.	Checkbox, optional field.
Linked Location Parent	Select this checkbox if the location is a Linked Location Parent.	Checkbox, optional field.
IPPBX Elements		
Voice Bandwidth (kbps)	This determines the voice bandwidth for the location.	Optional. Modify the required voice bandwidth for the location. This field is available only if the location is not sharing a Bandwidth Group. If 0 is entered, the bandwidth is unlimited.
Video Bandwidth (kbps)	This determines the video bandwidth for the location.	Optional. Modify the required video bandwidth for the location. This field is available only if the location is not sharing a Bandwidth Group. If 0 is entered, the bandwidth is unlimited. If -1 is entered, the bandwidth is none.
Critical Numbers		
Published Number	<p>The PSTN (E164/ Public Switched Telephone Network) number for the location. This number will be presented to the called party.</p> <p>This must be a National PSTN number with the leading digit dropped.</p>	<p>This is a read-only field.</p> <p>Depending on Caller Line ID rules, this number may be presented to the called party as the phone number of the caller.</p> <p>The PSTN Published number can be updated via the <i>Location Advance Management > PSTN Published Number</i> screens</p>

Field	Description	Remarks
Site Location Number	The internal Extension number for the location.	This is a read-only field. The Internal Published Number can be updated via <i>Location Advance Management > Internal Published Number</i> screens.
Emergency Number	The location emergency Number.	This is a read-only field. If applicable, this number is sent to the emergency services when an emergency call is done from the system. This allows the emergency services to call back to a number which should be always manned. The location Emergency Number can be updated via <i>Location Advance Management > Emergency Number</i> screens.
Default MoH Track	Music-on-Hold track.	Select from the drop-down list.
Media Services		
Name	Select the media service (if applicable).	Optional.
IP Address Allocation		
See: Manage Subnets on page 762		
Dial Plan Tools		
Dial plan name	Dial Plan associated with this location at the point the location was created.	This is a read-only field.
Hardware Group	Defines a set of hardware devices e.g. PBXs, Gateways on the network used by the location.	This is a read-only field.
PBX Template Chosen	The PBX template set to the location at the point the location was created.	This is a read-only field.
Default Area Code	The location national area code.	This is a read-only field.
RID Code	The relevant RID code.	This is a read-only field.
Extension Length	Number of digits for the internal phone numbers (extensions).	This is a read-only field.
Dial this to get outside line	Prefix used to enable outside dialing.	This is a read-only field.
Inter-Site Prefix	Inter-site prefix for the location.	This is a read-only field.
Local Dialling	Local dialling number of digits - 7 or 10.	This is a read-only field.
GUI Branding and Notes		
See: Additional Information on page 761		
Codecs		

Field	Description	Remarks
Intra-Region Max Audio Bit Rate	The Intra-Region Max Audio Bit Rate for the location.	<p>Next to the bit rate value is an indication of the level at which the location's codecs were set, i.e. Dial Plan, Customer or Location. This field is a read-only field. Once a location's codecs have been set, it can only be modified via <i>Location Administration > Administration Tools</i>.</p> <p>Note</p> <p>Codecs can only be set at the customer/building/location level, if the associated dial plan makes provision for it.</p>
Inter-Region Max Audio Bit Rate	The Inter-Region Max Audio Bit Rate for the location.	<p>Next to the bit rate value is an indication of the level at which the location's codecs were set, i.e. Dial Plan, Customer or Location. This field is a read-only field. Once a location's codecs have been set, it can only be modified via <i>Location Administration > Administration Tools</i>.</p> <p>Note</p> <p>Codecs can only be set at the customer/building/location level, if the associated dial plan makes provision for it.</p>

See also:

- [Adding a location on page 749](#).

Additional Information

Location additional information refers to details located at the bottom of the *Location Management* screen.

The information provided in this section is as follows:

Field	Description	Remarks
GUI Branding - default branding of User Interface	The default brand allocated to an end user when it is created in the system.	<p>Select from a drop-down list.</p> <p>The list of available brands is determined when a location is created.</p>

Field	Description	Remarks
Brands List	List of brands available at the location.	Each can be enabled/disabled by a checkbox. Each enabled brand can be allocated to an end user when it is created and the administrator wishes to allocate that user with a brand different from the default defined for the location.
Notes	Enter additional text as required.	This is an optional field.

Manage Subnets

An IP subnet is a logical group of IP addresses, normally based on the private address range within a provider or customer. The system enables a location to have multiple subnets. A single subnet can also be shared between two locations.

The system stores more information about managed subnets than unmanaged. This allows the system to ensure that elements of a managed subnet are used correctly in terms of networking. The system assumes that another server is controlling the elements of an unmanaged subnet.

Note

- If you do not fully understand IP addressing, we suggest that you read some additional background information before proceeding.
 - To find a particular subnet, the system provides users with an IP subnet search input text box and **Search** button.
-

Manage and control the location subnets (IP Addresses) from the *Location Management* screen.

Click the **Manage Subnets** button in the *IP Address Allocation* section of the *Location Management* screen. The *Manage Subnets* screen allows you to perform the following procedures:

- [Procedure 2, “Viewing location subnets” on page 762](#)
- [Assign managed subnets on page 764](#)
- [Add Unmanaged Subnet on page 764](#)
- [Procedure 3, “Releasing a Managed Subnet” on page 763](#)
- [Procedure 4, “Deleting an Unmanaged Subnet” on page 764](#)

Procedure

Viewing location subnets

To view locations subnets:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the *Location Name* (active text link) that you would like to modify.
- Step 3** Click the **Manage Subnets** button in the *IP Address Allocation* section on the *Location Management* screen. The *Manage Subnets* screen is displayed, where the existing subnets are shown along with the following information:

Field	What is it?	Updated?	Notes
IP Subnet	IP Address of the IP Subnet.	Read-only	The IP Address allocated to this subnet, for example 10.55.6.0.
Subnet Mask	The range of addresses available for this subnet.	Read-only	-
Location Used for Automove?	Y/N for use when location is allocated with a shared subnet.	Read-only	<p>Only applicable for shared subnets. When a regular (non-shared) subnet is used, this flag is always "Y".</p> <p>Shared subnet and use of Automove:</p> <p>Y- Should be set for only one location from the list of locations sharing the same subnet. The system moves the phone automatically into that location.</p> <p>N- Should be set for all other locations sharing the same subnet.</p>
Managed	Indicates whether the subnet is managed (Y) or unmanaged (N).	Read-only	-

[Assign managed subnets on page 764](#)

[Add Unmanaged Subnet on page 764](#)

Procedure

Releasing a Managed Subnet

Note

A managed subnet can be released from a location only if none of the IP Addresses it maintains are used in the location.

To release a managed subnet from a location:

- Click the **Release** button adjacent to the subnet you want to release.

Note

Releasing a subnet from the location only removes it from being available at the location. This subnet still exists in the system and can still be assigned to another location.

Procedure

Deleting an Unmanaged Subnet**Note**

An unmanaged subnet can be deleted from a location only if none of the IP Addresses it maintains is used in the location.

To delete an unmanaged subnet from a location:

- Click the **Delete** button adjacent to the unmanaged subnet you want to delete.
-

Add Unmanaged Subnet

Procedure

To add an unmanaged subnet:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the *Location Name*(active text link) to which you want to add an unmanaged subnet.
- Step 3** Click the **Manage Subnets** button in the *IP Address Allocation* section of the screen. The *Manage Subnets* screen is displayed.
- Step 4** Click the **Add Unmanaged Subnet** button. The *Add Unmanaged Subnet* screen is displayed.
- Step 5** Complete the required fields (see table below for details).

Field	Description
<i>IP Subnet</i>	Enter the IP address of the unmanaged subnet you wish to add. This is a mandatory field. When adding either a managed or an unmanaged subnet, the network address of the subnet (not the first usable IP or any other IP in the subnet) should be entered in the <i>IP Subnet</i> text box.
<i>Subnet Mask</i>	Enter the IP address of the unmanaged subnet you wish to add. This is a mandatory field.
<i>Use Location for Automove</i>	Select this checkbox if you would like to use the location for Automove

- Step 6** Click the **Add** button when complete. The unmanaged subnet is added to the location.
-

Assign managed subnets

Procedure

To assign a managed subnet to a location:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the *Location Name* (active text link) to which you want to add an unmanaged subnet.
- Step 3** Click the **Manage Subnets** button in the *IP Address Allocation* section of the screen. The *Manage Subnets* screen is displayed.

Step 4 Click the **Assign Managed Subnet** button on the *Manage Subnets* screen. The *Add Subnet* screen is displayed.

Step 5 Complete the required fields. The following details are available:

Field	What is it?	Updated?	Notes
Select Managed IP Subnet to assign to Location	The subnet to be added to the location.	Mandatory	Select from the drop-down list. The list displays the subnets not yet allocated to any location.
Use Location for Auto-move	Used to determine if you would like to use the location for Auto-move of phones.	Optional	Enable (select) or Disable checkbox as required.

Step 6 Click the **Add** button when complete. The managed subnet is added to the location.

Advanced Location Management

Advanced management for a location comprises two screens accessible from the main *Location Details* screen. Advanced Management is accessed by clicking the **Advanced Mgt.** button.

This screen provides the following options:

Option	Brief Description	Cross Reference
Billing Codes Management	Billing codes enable you to track calls by associating a billing code with each call.	Billing Codes Management on page 766.
PSTN Published Number	PSTN (Public Switched Telephone Network). This must be a National PSTN number with the leading digit dropped.	PSTN Published Number on page 767.
Internal Published Number	This is the internal extension number.	Internal Published Numbers on page 768.
Emergency Number	This is a call-back number for emergency services.	Emergency Number Management on page 770.
Voicemail Management	Voicemail allows callers to leave messages when a phone is unanswered or diverted to the voicemail system. It also allows users to retrieve voicemails.	Voicemail Management on page 775.
Auto Attendant	An automated attendant system transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator.	Auto Attendant Service Management on page 769.
Conference Service Mgt	Conference Services enable two or more users to participate in a conference call. This option enables administrators to manage the configuration and availability of the service.	Conference Services Connections on page 774.

Option	Brief Description	Cross Reference
Advanced Telephony Management	<p>This screen consists of a list of available advanced telephony features. Currently, the available settings include:</p> <p>FwdRedirectingExternalNumon-CallFwd</p> <p>Emergency CLI Preference</p> <p>Default SNR Rerouting CoS</p>	Advanced Telephony Management on page 771.
Directory Service Mgt	This screen enables you to manage the Directory Services for a location.	Location Directory Management on page 773.
Adjacent Area Code	<p>Geographic areas are often covered by a single area code that is then split into two or three codes. Once capacity is reached, certain sections retain the existing area code, usually the area with the highest customer density, while the remaining customers receive new area codes.</p> <p>Note</p> <p>The Adjacent Area Code button is only available for locations that are configured for 10-digit local dialing.</p>	Area Code Management on page 768.
GeoLocation	GeoLocations are treated as an attribute of a Location, and are automatically associated to or disassociated from a Location when added or deleted respectively. GeoLocations are mandatory for the Extension Mobility Cross Cluster (EM-CC) to function.	Geolocation Management on page 405.

When you select preferences, the list of location preferences screen appears (see [Location Preferences Management on page 779](#)).

Billing Codes Management

In some business environments, it may be necessary to bill individual calls to different accounts. This is often used in professional services businesses (for example lawyers' offices) where it is required to bill each return call to a customer's account.

This is achieved through the use of billing codes that are added to a call's Call Data Record (CDR).

Click the **Billing Codes Management** button on the *Advanced Location Management* screen. The available billing reference codes are displayed on the *Billing Reference Codes* screen.

The following functionality is available from the screen:

Button	Description	Remarks
Add Range	Allows the location administrator to add a range of numbers to a specific billing code and to select how many numbers to include in the range.	Reference codes need to be pre-defined. Ranges can be added in the following multiples: 1, 10, 20, 50, 100, 200, 500, or 1000
Delete Range	Allows the location administrator to delete a range of numbers in a specific billing code.	Enter the start billing code of the range you want to delete and select the size of the range to be deleted.
Assign Range	Allows the location administrator to assign a range of numbers to a specific billing code of the location.	Select the relevant level to assign the billing code to, for example Location or User. Enter the billing reference code and range size.
Release Range	Allows the location administrator to release a range of numbers in a specific billing code.	Use this button to release a previously assigned range.
Enable Range	Allows the location administrator to enable a range of numbers in a specific billing code.	Enable the range using the billing reference code.
Disable Range	Allows the location administrator to disable a range of numbers in a specific billing code.	Disable the range using the billing reference code.

To update billing codes, select the relevant *Billing Code* instance to manage. The following fields are available:

Field	Description	Remarks
<i>Billing Ref</i>	Billing reference number.	-
<i>Usage</i>	Indicates at what level the Billing code is assigned.	-
<i>Release/Assign</i>	Indicates if a billing code has been assigned or not. Toggle the active text link as required (Release/Assign).	-
<i>Instance</i>	Displays the details of the customer, location or user that the billing code has been assigned to.	If selected, it opens the management screen for the selected instance (user).
<i>Disabled</i>	Indicates if the billing code is enabled (N) or disabled (Y).	If the billing code is enabled, you can disable it by selecting the <i>Disable</i> active text link.
<i>Description</i>	Description of the billing code.	-

PSTN Published Number

Procedure

To manage the PSTN number for the current location:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the *Location name* (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **PSTN Published Number** button.

- Step 5** **Note:** Make sure that the correct format is used for this number, otherwise, certain calls to the PSTN (such as those from internal numbers) may fail. The required format is dependent on the configuration of your dial plan, see [Dial Plan Management on page 54](#).

To add a published PSTN number to the location, type the published PSTN number in the *Published PSTN Number* field and click the *Add* button.

To modify the existing published PSTN number of the location, edit the published PSTN number in the *Published PSTN Number* field as required and click the **Modify** button.

Click the **Delete** button to delete the published PSTN number.

The PSTN published number is updated.

Internal Published Numbers

Procedure

To manage the internal published number for the current location:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the **Location name** (active text link) that you would like to modify.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Internal Published Number** button.
- Step 5** To add an internal published number to the location, select it from the *Internal Published Number* drop-down list and click the **Add** button.

To modify the existing internal published number of the location, select the required number from the *Internal Published Number* drop-down list and click the **Modify** button.

Click the **Delete** button to delete the internal published number.

Area Code Management

Geographic areas are often covered by a single area code that is then split into two or three codes. Once capacity is reached, certain sections retain the existing area code, usually the area with the highest customer density, while the remaining customers receive new area codes. One benefit of a geographic split is that an area code remains defined as a geographic area; this enables customers to have a fairly good idea about the location of the person they are calling. A draw-back of a geographic split is that a large number of customers have to change their area codes.

The system enables administrators to define Adjacent Area Codes. Adjacent Area Codes are sometimes also referred to as Overlay Area Codes. Once this code has been configured, a user in these locations can make local calls to a phone in the Adjacent Area Code by dialing the External Prefix followed by NPA-NXX-XXXX, where NPA is the configured Adjacent Area Code.

Procedure

Adding an Adjacent Area Code

Note

Adjacent area codes can only be added to locations that are configured for 10-digit local dialing.

To add an Adjacent Area Code:

-
- Step 1** Browse to *General Administration > Locations*.
- Step 2** If required, select the required Provider and Customer.
- Step 3** Select the location to which you would like to assign an Adjacent Area Code. The Manage Location window appears.
- Note**
- To ensure that you are adding the Adjacent Area Code to the correct location, please review the location name displayed along the header of the screen.
- Step 4** Click the **Advanced Mgt.** button.
- Step 5** Click the **Adjacent Area Codes** button.
- Step 6** Click the **Add** button.
- Step 7** Specify the required *Adjacent Area Code*.
- Step 8** Click the **Add** button. The adjacent area code is added to the system.
-

Note

You need to repeat this procedure for all required Adjacent Area Codes and for all locations.

Procedure

Viewing Adjacent Area Codes

To view Adjacent Area Codes:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** If required, select the required Provider and Customer.
- Step 3** Select the location that you would like to view the Adjacent Area Codes for.
- Step 4** Click the **Advanced Mgt.** button.
- Step 5** Click the **Adjacent Area Codes** button. All Adjacent Area Codes for the selected location are displayed.
-

Auto Attendant Service Management

An automated attendant or Auto Attendant system transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator. This is achieved via a system of voice menus that the person initiating the call interacts with via their telephone keypad or via voice commands. In some Auto Attendant systems, there are message-only information menus and voice menus that are used so that an organization can provide business information such as hours, directions to their premises, information about job opportunities, and answer other frequently-asked questions. After the message has played, the caller can be forwarded to the receptionist or they can return to the main menu.

View and Modify an Auto Attendant Service

Procedure

To view and modify an *Auto Attendant Service*:

- Step 1** Browse to the required location.
- Step 2** Click the **Advanced Mgt.** button.
- Step 3** Click the **Auto Attendant** button.
- Step 4** Select the *Name* (active text link) of the *Auto Attendant Service* that you would like to view.
- Step 5** Modify the required fields, then click the **Modify** button. The details of the selected Auto Attendant service are updated.

To Manage an IVR's configuration, select the *Configure IVR* active text link. This link is only displayed if this functionality is available on your system.

Procedure

Delete an Auto Attendant Service

To delete an *Auto Attendant service* from the system:

- Step 1** Browse to the required location.
- Step 2** Click the **Advanced Mgt.** button.
- Step 3** Click the **Auto Attendant** button.
- Step 4** Click the **Delete** button adjacent to the *Auto Attendant Service* that you would like to delete, alternatively, select the *Auto Attendant Service Name* (active text link) that you would like to delete then click the **Delete** button.

After confirming the delete operation, the *Auto Attendant Service* is deleted from the location.

Add an *Auto Attendant Service* at the Location Level

Procedure

Note

Before adding an Auto Attendant service, please ensure that an Auto Attendant Server has been added.

To add an Auto Attendant Service at the location level:

- Step 1** Browse to the required location.
 - Step 2** Click the **Advanced Mgt.** button.
 - Step 3** Click the **Auto Attendant** button.
 - Step 4** Click the **Add** button.
 - Step 5** Complete all of the required fields then click the **Add** button. The Auto Attendant service is added to the location.
-

Emergency Number Management

An Emergency Responder ensures that emergency calls are sent to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.

Procedure

Adding an Emergency Number

To connect to an Emergency Number:

- Step 1** Browse to the required location.
 - Step 2** Click the **Advanced Mgt.** button.
 - Step 3** Click the **Emergency Number** button.
 - Step 4** Select the emergency number for the location from the drop-down list of PSTN numbers available in the location.
 - Step 5** Click the **Submit** button.
-

Procedure

Removing an Emergency Number

To disconnect an Emergency Number:

- Step 1** Browse to the required location.
 - Step 2** Select the **Advanced Mgt.** button.
 - Step 3** Click the **Emergency Number** button.
 - Step 4** Select the required *Emergency Number* from the drop-down list and then click the **Delete** button.
-

The Emergency Number is removed from the location.

Advanced Telephony Management

This screen consists of a list of available advanced telephony features. Currently, the available settings include:

- FwdRedirectingExternalNumonCallFwd
- Emergency CLI Preference
- Default SNR Rerouting CoS

FwdRedirectingExternalNumonCallFwd

The *FwdRedirectingExternalNumonCallFwd* setting is used to manage the *AssociateFNN-Redirect* and *DisassociateFNN-Redirect* transactions at the location level. This setting drives the use of the AssociateFNN-Redirect model. The purpose of the feature and model is to include a mapping in the TimesTen DB for calls being forwarded to the PSTN. In the case where the calling number matches an entry, its FNN would be used as the CLI for the call (instead of the default behavior of site published number).

The *DisassociateFNN-Redirect* setting is managed via a drop-down list. The following options are available from the drop-down list:

- Derived From Customer: This is the default setting. This setting is enabled or disabled based on the setting at the Customer level. This can be configured as described under [Advanced Telephony Settings on page 674](#).
- Enabled: Regardless of the setting at the Provider level, this feature is enabled for the Location.

- Disabled: Regardless of the setting at the Provider level, this feature is disabled for the Location.

Procedure

Modifying the Setting

To modify the *AssociateFNN-Redirect* setting:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Advanced Telephony Management** button.
 - Step 5** Select the required status from the drop-down list adjacent to the *FwdRedirectingExternalNumonCallFwd* option.
 - Step 6** Click the **Apply** button. After confirming the operation, the *AssociateFNN-Redirect* transaction is updated.
-

Emergency CLI Preference

The *Emergency CLI Preference* is used to manage the *Emergency CLI* behavior at the location level.

The *Emergency CLI Preference* setting is managed via a drop-down list. The following options are available from the drop-down list:

- Derived From Customer: This is the default setting. This setting is enabled or disabled based on the setting at the Customer level. This can be configured as described under [Advanced Telephony Settings on page 674](#).
- Emergency Number: Regardless of the setting at the Customer level, this preference uses the Emergency Number.
- Device CLI: Regardless of the setting at the Customer level, this preference uses the Device CLI.

Procedure

Modifying the Setting

To modify the *Emergency CLI Preference* setting:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select *Location Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Advanced Telephony Management** button.
 - Step 5** Select the required status from the drop-down list adjacent to *Emergency CLI Preference*.
 - Step 6** Click the **Apply** button. After confirming the operation, the Emergency CLI Preference is updated.
-

Default SNR Rerouting CoS

The *Default SNR Rerouting CoS* setting is used to configure the default rerouting CoS used for SNR profiles for this location.

Available values are the 'outbound' service types configured for the dialplan.

Procedure

Modifying the Setting

To modify the *Default SNR Rerouting CoS* setting:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Advanced Telephony Management** button.
 - Step 5** Select the required option from the drop-down list adjacent to the *Default SNR Rerouting CoS* option.
 - Step 6** Click the **Modify** button when complete. After confirming the operation, the *Default SNR Rerouting CoS* transaction is updated.
-

Location Directory Management

This screen enables you to manage the Directory Services for a location.

Procedure

Connecting to a Directory Service

To connect to a directory service:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Select the **Advanced Mgt.** button.
 - Step 4** Select the **Directory Services Mgt** button.
 - Step 5** Select the **Connect** button adjacent to the service that you would like the location to connect to.
-

The Directory service is connected to the location.

Procedure

Disconnecting from a Directory Service

To disconnect from a directory service:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Select the **Advanced Mgt.** button.
 - Step 4** Select the **Directory Services Mgt** button.
 - Step 5** Select the **Disconnect** button adjacent to the service that you would like the location to disconnect from.
-

The Directory service is disconnected from the location.

Location Conference Management

This section covers Conference Services connections and management.

Conference Services Connections

Conference Services enable two or more users to participate in a conference call. This option enables administrators to manage the configuration and availability of the service.

Procedure

To connect to a Conference service:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Conference Services Mgt** button.
 - Step 5** Select the required conference server from the conference service available at customer level drop-down list and then click the **Add** button. The conference service is added to the location.
-

Procedure

To disconnect from a Conference service:

- Step 1** Browse to *General Administration > Locations*.
 - Step 2** Select the *Location Name* (active text link) that you would like to modify.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Conference Services Mgt** button.
 - Step 5** Select the required Conference server from the Conference Service Available at Customer Level drop-down list and then click the **Delete** button.
-

After confirming the deletion operation, the conference service is removed from the location.

Manage Location Conference Service

The *Manage Location Conference Service* screen enables administrators to manage conference services at the location level. Administrators are able to add, delete and modify conference services

Procedure

Adding a Location Conference Service at the location level

To add a location conference service at the location level:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Click the **Advanced Mgt.** button.
- Step 3** Click the **Conference Service Mgt** button.
- Step 4** To add a conference service, click the **Add** button.

- Step 5** Select the required service from the drop-down list then click the **Add** button.

The Conference service is added to the system.

Procedure

Modifying a Conference Service at the location level

To modify a conference service at the location level:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Click the **Advanced Mgt.** button.
- Step 3** Click the **Conference Service Mgt** button.
- Step 4** Select the required service from the drop-down list then click the **Modify** button.

The Conference service is modified within the system.

Procedure

Deleting a Location Conference Service

To delete a conference service at the location level:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Click the **Advanced Mgt.** button.
- Step 3** Click the **Conference Service Mgt** button.
- Step 4** Click the **Delete** button.

Voicemail Management

To create a voicemail service within a location, a voicemail service with corresponding pilot number configured must be available for the customer or the provider.

To manage voicemail services for the location:

Select *Voicemail Management* on the *Advanced Location Management* screen. The *Voicemail Management* screen is displayed.

This screen displays the existing voicemail profile as well as the associated voicemail service name for the selected location. To manage an existing voicemail service, select the *Voicemail Service Name* (active text link) in the *Details* section of the screen.

If a voicemail service is not configured for the location, you are immediately prompted to add one via the *Add Location Voicemail Service* screen as follows:

Procedure

Adding a Location Voicemail Service

To add a voicemail service:

- Step 1** Enter a Name for the location voicemail service. This is a mandatory field.
- Step 2** Enter a Description (optional) for the location voicemail service.

- Step 3** Select a voicemail service from the drop-down list.
- Step 4** Click the **Next** button.
- Step 5** Select the voicemail pilot number from the drop-down list.

Note

The pilot number in this example is an internal extension number and not a DDI number. If an internal number is used, then users cannot dial into the Pilot number from a PSTN number to retrieve voicemail messages. The pilot number must be a DDI (E164) number for Users to dial into the number from off-site or mobile phones. The setup of the pilot number is done at the customer or provider level.

- Step 6** Click the **Add** button, or click the **Add and Enable** to add the voicemail service to the location and make the voicemail service available for all the phones, CTI devices and users already set up or configured at this location.

Note

If users/phones are already defined in the location you must use the **Add and Enable** option.

Managing Voicemail Profiles

The system enables locations to have multiple voicemail profiles associated to them. This functionality can be used in organizations that require locations to have multiple area codes per location and need this supported by voicemail. When specifying the voicemail profile, a voicemail box mask is entered. The voicemail box mask specifies the mask that is used to format the voicemail box number for phones.

When forwarding a call to a voice messaging system, the mask is applied to the voicemail box number configured for that line. For example, if you enter a voicemail box mask of 12345XXXX, the voice mailbox number for directory number 2222 becomes 123452222. If a voicemail box mask is not entered, the voicemail box number matches the directory number (for example, 2222).

Procedure

Adding a Location Voicemail Profile

To add a location voicemail profile:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the required *Location* (active text link).
- Note**
- Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.
- Step 3** Click the **Advanced Mgt.** button.
- Step 4** Click the **Voicemail Mgt.** button.
- Step 5** Click the **Voicemail Profile Mgt.** button.
- Step 6** Click the **Add** button.
- Step 7** Complete all of the required fields and click the **Submit** button.
-

The following table describes the fields available on the *Add Voicemail Profile* screen:

Field	Description	Remarks
Voicemail Name	This field cannot be modified and is displayed for information purposes only.	-
Voicemail Profile Name	The name of the voicemail profile being added.	This is a mandatory field.
Description	A description of the voicemail profile being added.	-
Pilot Number	This field cannot be modified and is displayed for information purposes only.	-
Box Mask	The voicemail box mask specifies the mask that is used to format the voicemail box number.	For example, if you enter a voicemail box mask of 12345XXXX, the voice mailbox number for directory number 2222 becomes 123452222. If a voicemail box mask is not entered, the voicemail box number is not modified in any way.

Procedure

Modifying a Location Voicemail Profile

To modify the details of a NAT subnet:

Step 1 Browse to *General Administration > Locations*.

Step 2 Select the required *Location* (active text link).

Note

Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

Step 3 Click the **Advanced Mgt.** button.

Step 4 Click the **Voicemail Mgt.** button.

Step 5 Click the **Voicemail Profile Mgt.** button.

Step 6 Select the *Name* (active text link) of the voicemail profile that you would like to modify.

Step 7 Make the relevant changes to the voicemail profile then click the **Modify** button. The profile is updated with the modifications.

Procedure

Deleting a Location Voicemail Profile

To delete a location voicemail profile:

Step 1 Browse to *General Administration > Locations*.

Step 2 Select the required *Location* (active text link).

Note

Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

- Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Voicemail Mgt.** button.
 - Step 5** Click the **Voicemail Profile Mgt.** button.
 - Step 6** Select the *Name* (active text link) of the voicemail profile that you would like to delete.
 - Step 7** Click the **Delete** button. After confirming the deletion, the voicemail profile is deleted from the system.
-

Managing Location Voicemail Profiles

The system enables you to specify a default voicemail profile for each location.

Procedure

To specify a default voicemail profile:

- Step 1** Browse to *General Administration > Locations*.
- Step 2** Select the required *Location* (active text link).

Note

Depending on where you are currently within the system hierarchy, you may need to first select the relevant provider, customer, reseller etc.

- Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **Voicemail Mgt.** button.
 - Step 5** Click the **Voicemail Profile Mgt.** button.
 - Step 6** Click the *Is Default* radio button adjacent to the location voicemail profile that you would like to set as the default.
 - Step 7** Click the **Modify** button. The selected profile is set as the default.
-

See also:

- [Managing Location Voicemail Profiles on page 778.](#)

GeoLocation Management

For Extension Mobility Cross Cluster (EMCC) to function, GeoLocations must be added to the locations at which EMCC is required. GeoLocations can also be modified or deleted as required.

Note

The **GeoLocation** button is **not** available if the cluster does not support EMCC or when using a Unified CM version lower than 8.0.

GeoLocations are automatically associated to or disassociated from a Location when added or deleted respectively.

If a location's cluster is EMCC-enabled, the location is, by default, associated with a geolocation on the cluster that uses the same country as the location. When the user views the geolocation, a message at the top of the page shows which cluster-level geolocation is currently associated. The **Add** button at the bottom of the page is also enabled.

Procedure

Adding a GeoLocation

- Step 1** Browse to *General Administration > Locations* at the Location level. The *Location Management* screen is displayed.
 - Step 2** Select the required *Location Name* (active text link). The *Manage Location* screen is displayed.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **GeoLocation** button. The *Add GeoLocation* screen is displayed.
 - Step 5** Enter the the required GeoLocation details, such as Name (mandatory), Description, Country Code, State, Region or Province (A1), County or Parish (A2), etc.
 - Step 6** Click the **Add** button when complete. The GeoLocation entry is added to the system.
-

Procedure

Modifying a GeoLocation

- Step 1** Browse to *General Administration > Locations* at the Location level. The *Location Management* screen is displayed.
 - Step 2** Select the required *Location Name* (active text link). The *Manage Location* screen is displayed.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **GeoLocation** button. The *Modify GeoLocation* screen is displayed.
 - Step 5** Edit the the required GeoLocation details, such as Name (mandatory), Description, Country Code, State, Region or Province (A1), County or Parish (A2), etc.
 - Step 6** Click the **Modify** button when complete. The GeoLocation entry is modified in the system.
-

Procedure

Deleting a GeoLocation

- Step 1** Browse to *General Administration > Locations* at the Location level. The *Location Management* screen is displayed.
 - Step 2** Select the required *Location Name* (active text link). The *Manage Location* screen is displayed.
 - Step 3** Click the **Advanced Mgt.** button.
 - Step 4** Click the **GeoLocation** button. The *Modify GeoLocation* screen is displayed.
 - Step 5** Click the **Delete** button. The selected GeoLocation entry is deleted from the system.
-

Location Preferences Management

Preferences allow customizations of locations on an individual basis. To view the available preferences, click the **Preferences** button from the selected *Location Details* page.

See [Available Preferences and Settings on page 934](#) if required for a list of available preferences for each location.

Modify Location Preference

To modify any preference setting, simply select the active text of the relevant preference. An example of how to modify a Location preference setting is shown below. In this case it is the 'AutoRegister'. This preference, when selected, allows the phone to automatically be registered when moved to this location.

To change the setting, select the **Current Setting** checkbox to enable the setting then click the **Modify** button.

Some preferences have values and not checkboxes. Enter the relevant details or select the required setting from the drop-down box then click the **Modify** button.

Phone Processes

Below is a list of the major processes which involve phones and affects its availability and status in the location.

There are three main types of activities which affect a phone in the location:

- **Inventory:** Availability of the phone in the location i.e. enables the phone device name to be recognized as one which belongs to the location. Inventory processes also support removing a phone from the location and returning it to the Provider inventory.
- **Registration:** Activate the phone to allow it to receive and make calls. Deregistration of a phone is also available as part of this set of processes (see [GUI Phone Registration on page 781](#)).
- **Management:** Handle (modify/update) phone after it is available and active allowing changes to some of their settings and features while in the location.

Note

Some changes may require the phone to be re-registered (unregistered then registered).

Phone in Location- Basic Terminology

Phone Status	Description?
Inventory	When a phone is initially entered into the system, it is added as an inventory item in the Service Providers warehouse. The device name and type are the only details known about the phone. Over time, the phone is allocated initially to a Reseller, who in turn allocates it to a Customer. It is still an inventory item. It does not become a provisioned phone until it has been allocated to a Location.
Provisioned	Once a phone has been moved into a Location and a specific subnet in it, the system allocates an IP address to the phone's device name. If that phone is physically connected onto the correct VLAN in that Location, then it is automatically provisioned with the allocated IP address.
Registered	Only a provisioned phone can be registered. The registering process provides the phone with a telephone number and a configuration file. Only a registered phone can operate as a normal phone and can make and receive calls.
Associated	An associated phone is linked to a user. That user becomes associated with the Phone's telephone number.
Logged on	Only a phone that has Extension Mobility Support can be logged onto by a user with User Mobility. Once logged-on, the phone adopts the profile of the Mobile User and drops their registered number and profile.

Phone Registration

Phone registration is the procedure of allocating a Class of Service (CoS) and number(s) to the phone.

Registration involves the re-booting of the phone by the system and a new, updated configuration file being sent to the phone.

Phone registration in the system can be done via three different routes.

	Phone Registration Methods	Cross Reference
1.	Manually via the system GUI	See GUI Phone Registration on page 781 .
		See Unregistering / Deleting a Phone on-page 820 .
2.	Automatic Registration by the system	See Automatic Registration on page 786 .
3.	Semi-Automatic using Phone XML services (Phone Based Registration)	See Phone Based Registration on page 788 .

Note

- When registering phones in an environment that has the Alerting Name functionality enabled, the *Alerting Name* field remains blank, and needs to be populated via the Phone Management section of the system. For more information on managing Alerting Names, see [Phone Alerting Names on page 818](#).
- The 3911, 3951, 6901 and 6911 phone types do not support extension mobility. To register these phones, the *Allow user login to phone* option in the phones' feature group must be disabled.

GUI Phone Registration

This process describes how a Location Administrator registers a new phone and assigns it with a phone number within the system GUI.

Note

It is recommended that immediately after registering the phone it should be modified. This allows for the configuration of all the phone and line settings and ensures that all system driven values are pushed to the Cisco Unified Communications Manager for that device. (The bulk loader and APIs for registering a phone have an automatic modify transaction after the register transaction as part of the registration workflow.)

Procedure

- Step 1** Select the *Phone Registration* option from the *Location Administration* menu.
- Step 2** Select the relevant *Location Name* (active text link). The list of phones provisioned in the location, and that are available for registration, appears:

Field	Description	Remarks
Phone Type	The Phone Type allocated in the system to this device name when the phone was added to the system Inventory.	This is a read-only field.

Field	Description	Remarks
IP Address	The IP address assigned to the phone when it was moved to the location.	This is a read-only field. Phones with an assigned IP Address are considered to be Provisioned.
Configuration Profile	Marks if the phone is a real phone (actual handset) or a Configuration Profile phone.	This is a read-only field. <ul style="list-style-type: none"> • N (Default) - real phone • Y - A configuration profile phone which is used for Phone Based Registration
Device Name	The name of the device.	This is a read-only field, and is an active text link used to register the device.
Device Group (Tenant)	If the phone is part of a device group, the name of the device group is displayed here.	This is a read-only field.

Step 3 Select the phone you want to register by selecting the *Device Name* active text link.

Phone Registration - Stage 1

Procedure

Step 1 Enter the required details. The following fields are available on the first screen when registering a phone:

Field	Description	Remarks
Phone Type	The type of the phone which is to be registered.	-
Device Name	The Phones Device name.	-
Description	A description for the phone being registered.	Enter the required description in the provided text field.
Softkey Templates	Softkey Template to be allocated to phone	Select from the drop-down list. The default is the 1st Softkey in the drop-down list Note If Feature Control Policies have also been allocated to the phone type, then softkey templates are not available to allocate to the phone.
SIP Profile	A Session Initiation Protocol (SIP) consists of a set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pick-up URI, and so on.	This is a mandatory field. Select from the drop-down list. This drop-down is only available when a SIP phone type is selected.

Field	Description	Remarks
Button Template Name	Button template allocated to phone.	<p>Note</p> <p>To make sure that the correct phone button templates are displayed, import the latest phone button templates from Unified CM as described in Importing/Refreshing CCM Items on page 87.</p> <p>Select from the drop-down list. The system automatically presents button templates based on the phone type selected.</p>
Phone Security Profile	Phone security profile allocated to phone.	<p>Note</p> <p>If CUCDM has no phone security profiles, the only available option in the drop-down list is <i>Use CUCM default</i>. This leaves the phone security profile as currently configured in Unified CM. To make sure that the correct phone security profiles are displayed, import them from Unified CM as described in Importing/Refreshing CCM Items on page 87.</p> <p>Select from the drop-down list. The system automatically presents phone security profiles that have been imported from Unified CM.</p>
First Expansion Module	Primary expansion module type to be used by phone.	<p>This is an optional field.</p> <p>This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.</p>
Second Expansion Module	Secondary expansion module type to be used by phone.	<p>This is an optional field.</p> <p>This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.</p>
Third Expansion Module	Third expansion module type to be used by phone.	<p>This is an optional field.</p> <p>This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.</p>
Feature Control Policy	The Feature Control to be allocated to the phone.	Select from the drop-down list. The default is the 1st Feature Control Policy in the drop-down list. This field is only available to certain device types.

Field	Description	Remarks
Media Services	Select the media service for the device.	The 'Derived from Location' option is the default option and is set to a media service associated with the location.
Device Group	Select the device group for the device from the drop-down list, which displays the device groups available at the location.	-
Select Phone Feature Group	Feature Group for the Phone.	<p>Select from the drop-down list.</p> <p>Only feature groups available from the relevant customer are available for selection.</p> <p>Note</p> <p>If a Feature Group is selected which makes provision for a feature that is not supported by the phone type, the Feature Group is still associated to the phone, but the end user encounters an error message when attempting to use the unsupported feature.</p>

Step 2 Click the **Next** button when complete. The Phone Registration (stage 2) screen is displayed:

Phone Registration - Stage 2

Procedure

Step 1 Enter the required details. The following fields are available on the second screen when registering a phone:

Field	Description	Remarks
Limits Outbound calls to	The Unified CM Class of Service from the feature Group.	-
Device Use	Is it a phone or a fax line?	Select from the drop-down list. Default = Phone.
SRST	Available if the phone has SRST enabled in its feature group.	Select the checkbox to enable SRST, and select the required SRST reference from the adjacent drop-down list, which also displays the remaining capacity as per existing functionality. The list of available device pools (see field below) is filtered based on the selected SRST reference.
Device Pools	The device pool to which the device is allocated.	Select the required device pool to allocate to the device from the list of available device pools at the location.

Field	Description	Remarks
Number Details - Line Number (line 1 to line n)	Phone Number.	<p>Select from the drop-down list.</p> <p>Default - the 1st number in the list.</p> <p>Numbers available in the list include (in ascending order):</p> <ul style="list-style-type: none"> • Available DDIs • Available Internal Extensions • Allocated Internal Extensions (to be shared) • Allocated DDIs (to be shared) • None - No phone number allocated to this line <p>Note</p> <ul style="list-style-type: none"> • Although shared analog lines can be allocated across all protocols, SIP and H323 may give unexpected results due to limited support in the Unified CM. • It is possible to register a phone with fewer lines than the maximum allowed. The maximum number of lines is determined by the number of feature group lines, phone button template lines, phone type lines and expansion modules selected. <p>If the first line of a SIP phone is empty (see also Manage Lines on page 810), Unified CM places the phone into an Unregistered state.</p> <p>Click the Clear Lines button to clear all settings.</p>
Number Details - Label (line 1 to line n)	Line label to appear on the phone.	<p>Enter the required label in the text field.</p> <p>The display name is derived from the line label.</p>

Field	Description	Remarks
Number Details - Line Class of Service	Line Class of Service for the phone.	Select from the drop-down list. Uses the Default Class of Service, as specified in the feature group, by default. Note Any changes to the feature group values or settings, whether modified in the Feature Group Management section or via Op-sTools, do not apply to the COS of a registered line.
Number Details - Button	The button numbers (when the phone has one or more expansion modules a separator line separates phone buttons from expansion module buttons).	The Button number as specified in the Button Template. Note The button display layout is dependent on: the importing of the button templates from Cisco Unified Communications Manager
Number Details - Button Type	The type of button.	The button type, as specified in the button template.

Step 2 Click the **Next** button when complete. The phone registration details are displayed on the screen.

Procedure

Phone Registration - Summary

Note

To prevent potential feature mismanagement, it is considered best practice to make sure that devices with shared lines belong to the same feature group.

Step 1 Review the registration details, and edit if required. Note that for *Number Details*, the *Number* cannot be entered on this page.

Step 2 Click the **Register** button when complete to register the phone at the location.

See also:

- [External numbers on page 826.](#)
- [Managing Available Internal Numbers on page 824.](#)

Automatic Registration

Automated Self-Registration of Phones is possible with the system. This involves the location phones being pre-loaded into the system's database.

Note

During the AutoCCMNewPhone process the MacToLocation transaction may be called. This auto-moves a phone to a Location based on IP Address and Location

associated IP Subnets. As part of this move to Location, the phone's device pool is set. Previously this was set to the one Device Pool per Location, but now that there could be multiple Device Pools, the process then uses the Default Device Pool as specified by the Location Administrator.

When the phone is plugged-in at any desk the system performs the following activities automatically:

- Discover that the phone is plugged in.
- Move it to the location and allocate it with an IP address from the location subnet.
- Register it with a predefined feature group and the next available number from a pre-configured list of numbers.

Once this is completed, the phone is ready for use. If required, users can subsequently log into the phone to confirm their phone association.

This auto-registration process greatly increases the capacity of Service Providers or Enterprises to roll out new sites.

There are four Location preferences (settings) relevant to automatic registration, as shown below.

- **AutoFeatureLocation:** Feature Group for automatic registration of phones for this location.
- **AutoRegister:** Automate the registration of phones at a location.
- **AutoMoveLocation:** Allow discovery and automatic move of Phones to this location (must be allowed at Customer level as well to take effect).
- **AutoRegisterLowestLocation:** Lowest extension number for allocation during the auto registration process in this location.

For further details about these preferences, see [Location Preferences Management on page 779](#).

A phone is 'valid' for Auto-Provisioning if the phone is assigned to a relevant Reseller, Customer or Division, as a parent to the Location.

Note

If the Phone is already assigned to a Location then it has already been provisioned by the system. A Phone is not 'valid' for Auto-Provisioning, if it is still in Provider inventory, or is in the unassigned status.

Procedure

To register a phone automatically:

- Step 1** Ensure the Location and Customer preference settings are set to true and the default settings are entered.
- Step 2** On connection to a Location Voice VLAN switch port, the IP phone sends DHCP Discover/ DHCP Request messages to the system's Voice-DHCP server(s) identified by the Voice IP Helper Addresses configured for the Voice VLAN.
- Step 3** Voice-DHCP server(s) respond to the DHCP Request message as follows:
 - Previously registered (valid) phones receive an IP address and associated DHCP options
 - Unregistered/Valid and Non-Valid phones are 'discovered' and processed by the system:
 - The system's DHCP server detects the IP address of the edge-router forwarding the DHCP request.

- The system's DHCP server queries the system server (providing the Device Name of the phone and IP address of the edge router).
- The system identifies the Location of the phone by reference to the list of IP addresses loaded into the system for valid Edge Routers/Subnets. (Note: These Edge Router IP addresses must be unique to a given subnet, in order to cater for Locations which have multiple subnets).

Step 4 If the phone is 'Valid' for Auto-Provisioning, AND Auto-Provisioning is enabled at the Location:

- The system 'Moves' the phone in the system Phone Inventory to the required Location, assign an IP address to the phone in the appropriate subnet, and configure the system's DHCP server to provide the relevant DHCP acknowledgment.
- The system also provisions the IP phone as an 'Un-Registered' device in the (CCM) IPPBX associated with the Location.
- If the phone is 'Not-Valid' for Auto-Provisioning, OR Auto-Provisioning is not enabled at the Location: The system does not configure the DHCP server and the phone does not receive a valid DHCP acknowledgment.

Step 5 Following successful Auto-Provisioning, the IP phone receives a valid IP address for its local subnet, receives the address of the relevant CCM TFTP server(s) in its DHCP options and then registers with the relevant CCM IPPBX Subscriber server(s). The phone shows 'Unregistered' in the Phone Mask and an internal only extension number on the 1st phone line.

Step 6 If a default Feature Group has been set in the *AutoFeatureLocation* preference and the default phone number pools set in the *AutoRegisterLowestLocation* preference, then the phone automatically registers with the respective default settings. Telephone calls can then be made on the registered phone.

Step 7 A Phone of Last Resort capability is provided by the system. If this setting is enabled, then the first phone connected to a subnet is allocated with the *AutoLastResortFeatureLocation* default number. The *Phone of Last Resort* feature is only specific to certain organizations.

Phone Based Registration

Phone Based Registration (PBR) differs from auto-registration in that PBR pre-configures phones using pre-configured, dummy, configuration profiles. Users can use either bulk loaders or the system GUI to add both actual and fake MAC addresses (phones) to the system. After loading the MAC addresses, users then finalize registration on their actual phones.

High level overview of PBR process

- A fake, or dummy, profile is created in the system with the *configuration profile* setting enabled.
- When the actual phones are connected to the network, the system adds the real phones to the inventory and moves them to the location based on their IP addresses, but does not register them with the location.
- The Administrator/End User then manually enters the *Primary line extension number* on the real phone through the *Phone Services* button.
- The fake Profile corresponding to the extension number selected by the user is then inked and downloaded on to the real Phone.

Note

- PBR is used during the roll-out phase when administrators know the actual MAC addresses of all the phones they want to place on users' desks, but don't know yet which user receives which phone.

- Administrators need to know each user's phone type, profile features and primary line extension number.
- If administrators do **not know** the actual MAC addresses of the phones to be deployed, they need to use the *auto-registration* feature and not the PBR feature.

Prerequisites

Before you can utilize the PBR feature, certain prerequisites need to be met:

- Ensure that the *XML-PhoneBasedProvisioning* customer preference is set to *True*. (To do this, browse to *General Administration > Customer*, then click the **Preferences** button on the relevant customer's page, before selecting the *XML- PhoneBasedProvisioning* active link and enabling the setting).

Adding Dummy (Fake) Phones

Dummy Phones are the fake phones that are created (or loaded) in the system and appear to have all the information as if they were *real* phones. However, the MAC address is not associated with an actual physical phone. Instead, a flag called *Configuration Profile* is set in the system to indicate that this is a fake phone. The phone-based registration process is based on the use of dummy (fake) phones.

We recommend that some form of standard naming convention for the MAC addresses of dummy phones is used to enable them to be easily managed and tracked.

For example "FAx..xy...y" (FA7961000001, FA0186000012, FA7970140003), where:

- FA = fake MAC address
- xxxx = phone type
- yyyyyy = counting the number of this fake phone type.

Dummy phones are added to inventory at the Provider level. The process for loading dummy phones is identical to adding real phone and they can be added either via the bulk loaders (see [The PBR Process Using Bulk Loaders on page 789](#)) or the system GUI (see [The PBR Process Using the system GUI on page 795](#)).

The PBR Process Using Bulk Loaders

Due to the average number of phone deployments during the PBR process, this process is almost always carried out via the Bulk loaders. However, alternate instructions are included at the end of this section that outline the use of the system GUI during PBR.

Procedure

To utilize PBR via the bulk loaders:

- Step 1** Use the *Add Move Phones* worksheet (in the LocAdmin workbook) to add the dummy MAC addresses. All of the associated information (phone types, button templates, COS, and so on) should be identical to the phone settings that are ultimately associated to the users.
- Step 2** Make sure that for each dummy MAC, you place a *Y* (for Yes) under the *Configuration Template* column (the default is blank for No).
- Step 3** Load the *Add Phones* worksheet into the system:

- Step 4** Move the dummy phones to their respective locations using the *Move Phones to Locations* worksheet (in *LocAdmin* workbook). Make sure you use the dummy MAC addresses (however, phone types and other data should match what you want to deploy to the user). Load the *Move Phones to Locations* worksheet into the system.
- Step 5** Register the dummy phones by using the *Register Phones* worksheet (in *LocAdmin* workbook) to load the dummy MACs. All the associated information (phone types, button templates, COS, extensions, etc) should be identical to the phone settings that are ultimately associated to the users.

Load the *Register Phones* worksheet into the system. The phones are placed in service and registered as dummy phones.

Note

The dummy phones are assigned the necessary extensions, which are used by the end users to register the real phones (see Step 13).

Notice that the dummy configuration profiles have been added to the system. The actual MAC addresses of each phone are unknown until the phones are placed on the users' desks:

Also note that the system provisions the dummy profiles in the Unified CM in the correct Device Pool. (The Device Pool is associated with the Device Pool of the location.)

- Step 6** Use the *Add Move Phones* worksheet (in the *LocAdmin* workbook) to add the real MAC addresses. All of the associated information (phone types, button templates, COS, and so on) should be relevant to the phone.
- Step 7** Make sure that for each MAC, you leave the *Configuration Template* column blank (the default is blank for No). Load the *Add Move Phones* worksheet into the system:
- Step 8** Move the real phones to their respective locations using the *Move Phones to Locations* worksheet (in *LocAdmin* workbook). Make sure you use the real MAC addresses. Load the *Move Phones to Locations* worksheet into the system.

Users must now replace the *dummy* MACs with the *real* MACs and register the desk phones with the actual MAC address and other settings. Notice that the system has auto-discovered this phone and provisioned it as an unregistered device with a temporary line number.



- Step 9** Select the *Services* menu item on the phone. The following screen is displayed:



Step 10 Select the *Phone Services* menu item (a system-generated phone XML feature). The following screen is displayed:



Step 11 Select the *Select Configuration Profile* menu item. The following screen is displayed:



- Step 12** If the configuration profile and the physical phone are in the same Location, enter the *primary extension number* of the first line on the selected configuration profile (in this example 1101) and click the **Submit** button.



If the configuration profile and the physical phone are not in the same location (this is relevant in network roll-outs where subnets are shared across more than one location) then enter the full DID number of the first line on the selected configuration profile.

The DID number is split into three sections:

- Country Code (the number you dial from outside the country to reach this line - in this example 971)
- National Code (the area code you dial - in this example 4)
- Local Number (in this example 6337122)

Click the **Submit** button.

Note

If data is entered in the Primary Line Number field and the DID fields (Country Code, National Code and Local Number) then the system only uses the data in the DID fields. In this case the Primary Line Number field is ignored.



- Step 13** The system reconfigures the phone with the details of the configuration profile phone, in effect, replacing the configuration file MAC address with the actual phone MAC.



- Step 14** The system unregisters the configuration profile phone and moves it out of the location (to the service provider level). After the first process, where only the extension is entered, the phone displays the following screen:



Within the system, the Phone Management screen displays the phone that has been provisioned.

Menu		Phone Management						
Setup Tools		Ref: [?]	Provider	Customer	Division	Location	User	Role
Dial Plan Tools		HCs_Provider	Reseller	Customer_1	Division_1	Location-111	bram Voss	Internal System SuperUser
Provider Administration		Search for Registered Phones for Location						
Networks		Search by	Device Name ends with	Max results	50			Search
Resources		Search results:						
General Tools		Select Phone						
General Administration		Phone Type	Usage	Device Name	First Line ExtLabel	Device Group	Configuration Profile	Associated User
Location Administration		Cisco ATA 186	Phone	ATA186556C15AA	/	N		702079@heagroup
Switchboards		Cisco ATA 18T SP	Phone	ATA186556C20AA	/	N		702080@heagroup
Telephony		Cisco Dual Mode for Android	Phone	D0702ALANDR1	/	N		702087@heagroup
Hunt Groups		Cisco Jabber Client	Phone	CJABBER1	/	N		702112@heagroup
Number Groups		CUCMCONNECT	Phone	CSPCucmconnect	/	N		702050@heagroup
Pickup Groups		CUCMOC	Phone	CSPCucmoc	/	N		702052@heagroup
End Users		Cisco Jabber M	Phone	MJABBER1	/	N		702113@heagroup
Phone Inventory		Cisco IP Communicator	Phone	IP_COMM1	/	N		702082@heagroup
Phone Registration		Cisco IP Communicator SIP	Phone	IP_COMM_SIP1	/	N		702083@heagroup
Phone Management		Cisco 8961 SP	Phone	SEP0028080CASA	1801 /	N		702199@heagroup
		Cisco 8961 SP	Phone	SEP0028080CASA	1803 /	N		702199@heagroup

In addition, Unified CM displays the phone as a registered member of the relevant Device Pool:

As for the second scenario that utilizes a shared subnet where the full DID number is entered, the phone displays the following screen:



The PBR Process Using the system GUI

Due to the average number of phone deployments during the PBR process, this process is almost always carried out via the Bulk loaders. However, alternate instructions are included here to outline the use of the system GUI during PBR.

Procedure

To utilize PBR via the system GUI:

- Step 1** Browse to Location Administration > Phone Inventory.
- Step 2** Click the **Add** button.
- Step 3** Enter the MAC Address, for example, in the format of "FAx.xy...y" (FA7961000001, FA0186000012, FA7970140003 etc.)
- Step 4** Select the required *Phone Type*.

- Step 5** Select the *Configuration Profile* checkbox.
- Step 6** Click the **Add Phone** button to add the phone to the inventory.
- Step 7** To move the dummy phone to the respective location, select the phone's *Device Name*.
- Step 8** Select the required *Move Target* then click the **Next** button.
- Step 9** Select the required *Subnet*, and the *Button Template*.
- Step 10** Click the **Move Phone** button.
- Step 11** To register the dummy phone, browse to *Location Administration > Phone Registration*, and then select the phone's *Device Name*.
- Step 12** Complete the required fields then click the **Register** button.
- Step 13** To add the real MAC address, browse to *Location Administration > Phone Inventory*.
- Step 14** Click the **Add** button.
- Step 15** Enter the real MAC Address for the phone.
- Step 16** Select the required *Phone Type*.
- Step 17** Do not select the *Configuration Profile* checkbox.
- Step 18** Click the **Add Phone** button to add the phone to the inventory.
- Step 19** To move the real phone to the respective location, select the phone's *Device Name*.
- Step 20** Select the required *Move Target* then click the **Next** button.
- Step 21** Select the required *Subnet* and *Button Template*.
- Step 22** Click the **Move Phone** button.

Users must now replace the *dummy* MACs with the *real* MACs and register the desk phones with the actual MAC address and other settings. Notice that the system has auto-discovered this phone and provisioned it as an unregistered device with a temporary line number.



Step 23 Select the *Services* menu item on the phone. The following screen is displayed:



Step 24 Select the *Phone Services* menu item (a system-generated phone XML feature). The following screen is displayed:



Step 25 Select the *Select Configuration Profile* menu item. The following screen is displayed:



- Step 26** If the configuration profile and the physical phone are in the same Location, enter the *primary extension number* of the first line on the selected configuration profile (in this example 1101) and click the **Submit** button.



If the configuration profile and the physical phone are not in the same location (this is relevant in network roll-outs where subnets are shared across more than one location) then enter the full DID number of the first line on the selected configuration profile.

The DID number is split into three sections:

- Country Code (the number you dial from outside the country to reach this line - in this example 971)
- National Code (the area code you dial - in this example 4)
- Local Number (in this example 6337122)

Step 27 Click the **Submit** button.

Note

If data is entered in the Primary Line Number field and the DID fields (Country Code, National Code and Local Number) then the system only uses the data in the DID fields. In this case the Primary Line Number field is ignored.



- Step 28** The system reconfigures the phone with the details of the configuration profile phone, in effect, replacing the configuration file MAC address with the actual phone MAC.



- Step 29** The system unregisters the configuration profile phone moves it out of the location (to the service provider level). After the first process, where only the extension is entered, the phone displays the following screen:



Within the system, the Phone Management screen displays the phone that has been provisioned:

Menu

- Setup Tools
- Dial Plan Tools
- Provider Administration
- Network
- Resources
- General Tools
- General Administration
- Location Administration
 - Switchboards
 - Telephony
 - Hard Groups
 - Number Groups
 - Pickup Groups
 - End Users
 - Phone Inventory
 - Phone Registration
 - Phone Management

Phone Management

Ref: [?view=phone&index=0]

Provider	Reseller	Customer	Division	Location	User	Role
HCS_Provider	Reseller_1	Customer_1	Division_1	Location-111	bwam Voss	Internal System SuperUser

Search for Registered Phones for Location

Search by Device Name ends with Max results: 50

Search

Search results:

Select Phone

Phone Type	Usage	Device Name	First Line ExtLabel	Device Group	Configuration Profile	Associated User	IP Address	Service Status
Cisco ATA 196	Phone	ATA768E58C1FAA	/	N	N	7002079@testgroup	10.55.1.175	Out of service(maintenance)
Cisco ATA 19T SP	Phone	ATA708E58C20AA	/	N	N	7002080@testgroup	10.55.1.176	In service
Cisco Dual Mode for Android	Phone	DOT204A-AMDR1	/	N	N	7002081@testgroup	10.55.1.163	In service
Cisco Jabber Client	Phone	CLJABBER1	/	N	N	7002112@testgroup	10.55.1.204	In service
CUCMCONNECT	Phone	CSPCucmconnect1	/	N	N	7002053@testgroup	10.55.1.15	In service
CUCMOC	Phone	CSPCucmocl	/	N	N	7002052@testgroup	10.55.1.149	In service
Cisco Jabber IM	Phone	MJABBER1	/	N	N	7002113@testgroup	10.55.1.205	In service
Cisco IP Communicator	Phone	IP_COMM1	/	N	N	7002063@testgroup	10.55.1.193	In service
Cisco IP Communicator SP	Phone	IP_COMM_SP1	/	N	N	7002062@testgroup	10.55.1.194	In service
Cisco 8961 SP	Phone	SEP0026080CA3C	1801 /	N	N	7001990@testgroup	10.55.1.19	In service
Cisco 8961 SP	Phone	SEP0026080CA5A	1803 /	N	N	7001991@testgroup	10.55.1.190	In service

In addition, Unified CM displays the phone as a registered member of the relevant Device Pool:

As for the second scenario that utilizes a shared subnet where the full DID number is entered, the phone displays the following screen:

Deployment Guide for Cisco Unified Communications Domain Manager 8.1.4 ER2

802



See also:

- [External numbers on page 826.](#)
- [Managing Available Internal Numbers on page 824.](#)
- [GUI Phone Registration on page 781.](#)
- [Location Preferences Management on page 779.](#)
- [Phone Inventory on page 830.](#)

Phone Management

This process describes how a Location Administrator can manage a phone after it has been registered. A registered phone is always associated with a specific location.

Note

Phones may automatically reset when certain configuration changes are made. This is a soft reset and shouldn't take more than a few seconds. If you would like to do a hard reset, click the **Phone Reset** button from the *Manage Phones* screen, this performs a hard reset and may take a number of minutes to complete.

There are several ways to find a specific phone after it was registered:

- Via Phone Management at the location level (*Location Administration > Phone Management*).
- Via Phone Inventory at the location level (*Location Administration > Phone Inventory*). See ???.

- Via Phone Inventory at the resources level (*Resources > Phone Inventory*). See ???.

Note

This process displays only phones that are registered in the location. For unregistered phones, see [GUI Phone Registration on page 781](#).

Procedure

Phone Management Search

Step 1 Browse to *Location Administration > Phone Management*.

Step 2 To find a specific phone or reduce the population displayed, select the search criteria from the *Search by* drop-down list, and type as many characters as you know in the field provided and then click the **Search** button. The following search criteria are available:

- *Device Name starts with:* One or more characters from the start of the phone device name
 - *Unregistered:* Phones which are allocated to the location but are not yet registered
 - *Registered:* Phones which are registered in the location
 - *Device name ends with:* One or more characters at the end of phone device name
 - *Phone Type:* The list of phones by phone type (need the full phone type if criteria is filled)
-

Note

The search string is not case-sensitive.

The list of phones registered in the location that match the selected search criteria is displayed on the screen, with the following details (see table below).

Field	Description	Remarks
Phone Type	The type of Phone.	-
Usage	How the device is configured.	Phone or Fax.
Device Name	The phones device name.	Active text link. Selecting the active text link allows you to manage the specific phone.
First Line Ext/Label	Information from the 1st line of the phone if registered.	Label is shown if it is not set to default.
Device Group	Device Group associated with the phone.	-
Configuration Profile	Configuration profile associated with the phone.	-
Associated User	Details of the end user associated with the phone.	Active text link. Selecting the active text link opens the User Management screen of that particular end user allowing you to manage that end user.
IP Address	The IP Address allocated to phone when it was provisioned in the location.	-

Field	Description	Remarks
Service Status	Indicates if the phone is in operational use or not.	<p>Active text link.</p> <ul style="list-style-type: none"> <i>In Service</i> - Phone available for service. Selecting the active text link takes the phone out of service. <i>Out of Service</i> - Phone not available for service. Selecting the active text link places the phone In Service. <i>Partially out of service</i> (limited calling options) - If the first line of the phone is suspended (using Operations Tools/<i>Suspend All Phones At Location Out of Service/First Phone Line Only</i> checkbox), then the first line of the device is not available for service and cannot be used currently. Selecting the active text link puts the phone back into <i>In Service</i> mode. <p>Note</p> <ul style="list-style-type: none"> After running the Ops Tool with the <i>First Phone Line Only</i> checkbox selected, then unsuspending the phone from the phone management page, if you then resuspend the phone, a full out of service is triggered, not the first line only. If a first line suspend is run directly after a full suspend, only the first line on the phone is suspended.

For information on Phone Registration, please see the [Phone Inventory on page 830](#) page.

Location Administration Tools

An administrator with the *LocationTools* permission (as set in the administrator's Access Profile) has access to and can execute *Location Administration > Administration Tools*.

Location Administration Tools allow for the automation of multi-step processes, such as resetting all phones in a location. The following location administration tools are available:

Operations Tool	Description	Remarks
Location Level		
Logout all extension mobility (roaming) end users of a location from all phones.	Logs out all roaming end users in a location from their phones.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the active text link, click the Submit button once you are sure you would like to proceed.</p>

Operations Tool	Description	Remarks
Reset all phones at a location	Resets all phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the active text link, click the Submit button once you are sure you would like to proceed.</p>
Set Location Codecs	Sets the Location Codecs for the <i>Intra-Region Max Audio Bit Rate</i> and the <i>InterRegion Max Audio Bit Rate</i> .	Use the drop-down lists to select the <i>Intra-Region Max Audio Bit Rate</i> and the <i>Inter-Region Max Audio Bit Rate</i> then click the Submit button.
Voicemail Caller Input Extension Search	<p>Caller input settings define actions that Cisco Unity Connection takes in response to the phone keypad keys that are pressed by callers during a user greeting.</p> <p>The Voicemail Caller Input Extension Search feature allows an administrator to replace existing extensions that are associated with specific keys.</p>	Enter the new extension in the <i>Replace with Extension</i> field and then click the Replace All button.

See the table under [Operations Tools on page 515](#) for a list of available operations tools.

Managing the Phone

Phone Details

This section contains static information about the phone such as the device name, phone type, IP address, feature group, description, default music on hold track, associated user, and configuration profile (Y or N). It also displays user configurable phone information such as button template name, device calling search space name (select the *Use default global settings* option when CSS must be provisioned as before), SIP profile (for SIP phone types only), soft key template, feature control policy, phone security profile, phone locale, idle URL, idle timeout and media services. To make sure that the correct phone security profiles are displayed, import them from Unified CM as described in [Importing/Refreshing CCM Items on page 87](#). Note that the fields available on this screen depend on the device type selected. Additional fields and checkboxes are available for the IMS-integrated mobile device, these include the Third-Party Registration Required and Block Incoming Calls checkboxes as well as the Home Network ID text field (maximum 255 characters) associated with the latter. These fields are only visible when the associated checkboxes are selected on the relevant Phone Type settings screen (see [Adding a Phone Type on page 39](#) for details). Enabling these checkboxes/fields provisions the associated feature on the Unified CM.

Calling search space (CSS) on a per-device basis can now be provisioned via the CUCDM. To set the device CSS on a per-device basis, the available CSS's must be preloaded as service types in the *handset_css* category. The *Device CSS Configurable* setting must be enabled in the CUCDM phone type settings. The description of the preloaded service types is available for selection (by the administrator) during phone registration and phone management.

The following buttons are available (depending on the configuration of the phone):

- **Phone Status** - click this button to display the phone status information sourced directly from the phone. If IP access is not available to the phone, no phone status is returned. Only available to phones connected to an IP subnet. If the phone is not reachable from the workstation that CUCDM is accessed from (due to NAT or firewall), then no status page is loaded. The error message that is shown is dependent on the user's browser and cannot be monitored or controlled by CUCDM.
- **Phone Reset** - click this button to clear faults on the line and rectify phone-based issues. (The **Phone Reset** function executes the **Unified CM Restart** function.)
- **Replace Phone** - click this button to replace a phone with another phone, while retaining all of the original settings - see [Replace a Phone on page 819](#).
- **Login/Logout User** - click this button to either login or logout a user to/from a phone remotely. Note that when using the Unified CM extension mobility service (BVSMRoaming = Off), user data displayed by CUCDM may be not be accurate since the login/out activity is handled directly by Unified CM. Any users logged in via CUCDM using this function are not subject to any login duration timers in Unified CM due to Unified CM interface restrictions - see [Login User on page 818](#).

Phone Layout

Note

This section is based on the button display layout and only appears in this format when button templates are imported from Cisco Unified Communications Manager (Unified CM).

The available buttons, with the associated button type and line details are listed. When the phone has one or more expansion modules, a separator line separates phone buttons from expansion module buttons.

Note

If the first line of a SIP phone is empty (see also [Manage Lines on page 810](#)), Unified CM places the phone into an Unregistered state.

Detailed information about the line associated with each button is displayed under the Settings (per Line) section (see [the section called “Settings \(per Line\)” on page 808](#)), e.g. Line1, Line 2, and so on. Select the *Line* active text link next to the relevant button to jump to the selected line details.

The following buttons are available:

- **Manage Lines** - click this button to access the Line Management screen, where you can add or delete lines as well as change the order of lines - see [Manage Lines on page 810](#) for more detailed information.
- **Manage Speed Dials** - click this button to configure the speed dial numbers for each phone - see [Manage Speed Dials on page 814](#) for more detailed information.
- **Manage Busy Lamp Fields** - click this button to manage the busy lamp fields for the phone - see [Busy Lamp Fields on page 815](#) for more detailed information.
- **Manage Service URL** - click this button to manage the Service URL associated with the phone - see [Manage Service URL on page 817](#) for more detailed information.

IP Phone Service Subscriptions

This section allows you to manage the phone's subscriptions to IP Phone Services. Click the **IP Phone Services** button to access the *Manage IP Phone Service Subscriptions* screen.

Phone Feature

This section allows you to manage the features available on the phone. Select the checkboxes adjacent to the features that you would like to activate. Features include: Allow user login to phone, Logout from hunt groups, Cache username on phone, and SRST. Adjacent to the *SRST* checkbox, there is a hidden SRST Reference field, and then beneath them the Device Pools field in the Device Pools section, which lists all Device Pools for the phone's Location. The hidden SRST Reference field is displayed when the SRST checkbox is selected (enabled). If SRST is enabled, then the SRST Reference filters the contents of the Device Pool field to include only Device Pools that use that SRST Reference. The inverse is true: when SRST is not selected the drop-down is filtered to include only non-SRST Device Pools (see also *Device Pools* field in the Device Pools section below). For more information on phone features, refer to [Feature Group Management on page 500](#).

Device Pools

The Device Pools section lists all the device pools available at the location. Change the device pool if required by selecting from the drop-down list (see also *SRST* option in Phone Feature section above).

Advanced Phone Settings

This section allows you to set the advanced phone settings imported from Cisco Unified Communications Manager (Unified CM) - see the Advanced Phone Settings document .

Click the *Advanced Phone Settings* heading to expand or collapse the list of available settings. The settings displayed are dependent on the advanced settings imported from the connected Unified CM. Next to each advanced setting, if available, the user can mouse-over a tooltip that provides more information about the setting.

Settings (per Line)

This section enables you to configure lines at a more detailed level. It lists all of the lines associated with the phone and enables you to modify the line settings for *Private line settings*, *Common line settings*, and *Common line settings (Call Forward)*. These settings include Label, ASCII Label, Message waiting lamp policy, Ring setting-(active and idle), Contact Center, Display name, ASCII Display Name, Call forward settings, Forwarded Call Display settings, Music on hold, Line Class of Service, and so on. You can configure aspects such as call forwarding and line labels, display names, alerting names and the ASCII value fields for label, display and alerting name fields. The fields displayed in this section vary according to the associated feature group's settings. For example, some phone types support *Recording Profile* and *Recording Option* settings so that if the recording profile has been imported ([Importing/Refreshing CCM Items on page 87](#)), it is available on the drop-down list. The *Recording Option* list has the following options, in accordance of the version of Unified CM:

- *Call Recording Disabled* - Unified CM 7.0 up
- *Automatic Call Recording Enabled* - Unified CM 7.0 up
- *Application Invoked Call Recording Enabled* - Unified CM 8.0 up
- *Device Invoked Call Recording Enabled* - Unified CM 7.0 up

The *Forward All Secondary CoS* field in the *Common line settings..... (Call Forward)* section of the screen is only visible if the *Forward All* checkbox is selected in the *Common Line settings(Call Forward)* section of the screen in the associated feature group.

Note

Text typed in the *Label* field automatically populates the *Label ASCII* field with the same text, it also overwrites any existing text in the *Label ASCII* field. You

can however edit text in the *Label ASCII* field without affecting/overwriting the text in the *Label* field.

When a Voicemail account is added to a user/line, call forward to Voicemail is enabled if no explicit call forward destination (number or URI) has been configured, that is the following Voicemail checkboxes in the *Common line settings for line n (Call Forward)* section of the screen are automatically enabled (set to true) on the selected line: *Forward Busy* (Int/Ext if applicable), *Forward No Answer* (Int/Ext if applicable), and *Forward Unregistered* (Int/Ext if applicable) if the corresponding destination field is left blank, that is no number or URI is configured [in the *Common line settings for line n (Call Forward)* section of the screen]. When a Voicemail account is added to a user/line, and the corresponding **destination has been configured** then the call forward settings on the line are left unchanged.

For shared lines, each feature listed in the Private Line settings section (now labeled Private line settings and Shared device settings) will be associated with a checkbox that can be selected to apply private line settings to all devices on the shared line. After the selection of the required checkboxes, click the **Apply** button.

Note

- To prevent potential feature mismanagement, it is considered best practice to make sure that devices with shared lines belong to the same feature group.
 - Shared line support for additional services in CUCDM, for example SNR, Presence, extension mobility, and so on, is dependent on Unified CM support. Make sure that the Unified CM you are using supports the features for the lines before attempting to provision them.
-

Example of copying a private line setting:

If the admin user enters a new value ("Line1") into the Label field (but does not modify this device first) and selects the Label and Line Mask checkboxes to change their values, the Label value changes to "Line1" and the Line Mask value also changes to the existing blank value for all devices on the shared line. Please note that the devices need not be associated to the user. Their private line settings are changed if they share the same extension. Also note that the **Apply** button is disabled (i.e. greyed out or not clickable) until one of the checkboxes is selected. If no checkbox is selected it remains disabled. The Apply button only change the private line settings for the current displayed line. It does not affect any of the other lines of the device. It is therefore not possible to select multiple settings on multiple shared lines and expect them all to be applied to all the shared lines.

For more information on line features, refer to [Feature Group Management on page 500](#).

Note

The call forwarding options set in the system are automatically provisioned as call forwarding options in Unified CM. However, if the checkbox for any call forward to Voicemail scenario is enabled, but a destination number or URI for the corresponding scenario is also provided, then both are provisioned on Unified CM, but the call forward to Voicemail setting overrides the destination number or URI.

Notes for managing lines that are cloned:

- All call forward and call forward voicemail settings are provisioned for all clones EXCEPT for 'call forward busy' and 'call forward busy to voicemail', which are **only provisioned on the last clone**.
- Line settings can only be changed for the original line, not the clones.

- All line settings changed for a line, automatically apply for the clones of that line, if any.
- Line details are suffixed with "(Clone)" if the line in question is a clone.
- When adding a new line to an already registered phone, the user has the option of cloning the new line.
- Individual clones cannot be deleted from a registered phone.
- When a line is deleted from a registered phone, any and all clones of that line are deleted as well.
- Lines listed for deletion that have clones will be suffixed with "Cloned(x)" where "x" represents the amount of clones.

Multiple Call/Call Waiting Settings for line. The following fields are displayed:

- Call waiting busy trigger
- Cloned Lines
- Max calls waiting

See also:

- [Phone Alerting Names on page 818](#)
- [Contact Center Agent Lines on page 819](#)

Additional Buttons

The following buttons are available at the bottom of the screen:

- **Modify** - click this button to update the phone details in Cisco Unified Communications Domain Manager (CUCDM).
- **Sync with Call Manager** - If there is no connectivity between the system and Call Manager, then an error message is displayed next to the *Call forward all calls to voicemail* field in the relevant common line settings section, informing you that these values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the page. Click the **Sync with Call Manager** button to manually sync these values with Call Manager when connectivity has been restored. The *Call forward - always* value is synced in a similar manner to the *Call forward all calls to voicemail* field.
- **Unregister** - click this button to remove the lines and all configured features from the phone - see [Unregistering / Deleting a Phone on page 820](#). Note that when a phone is unregistered, it is automatically placed into the location's default device pool.

Manage Lines

This section enables you to manage the lines for a phone, including to allow admin users the ability to reorder one or more lines or clones.

Procedure

Lines can be managed as follows:

- Step 1** Click the **Manage Lines** button on the *Phone Management* screen for the required device. The *Line Management* screen is displayed.
- Step 2** Complete the *Number Details:* section of the screen. The following fields are available:

Field	Description
<i>Button #</i>	The configured button # for the selected device is displayed.
<i>Line</i>	Lists extensions and numbers configured for the corresponding button # position. This field has a checkbox to provide the user the ability to move and delete multiple lines together. This field is also selectable; once selected all lines associated are highlighted in bold allowing the user to easily identify associated extensions.
<i>Action</i>	<p>Two action buttons are displayed depending on the current line position configuration. An Add button is displayed adjacent to the <i>Button #</i> if no number has been configured for the position. A Delete button is displayed adjacent to the <i>Button #</i> if a number is configured for the button. This allows for the number to be easily removed. See under <i>Add Line</i> and <i>Delete Line</i> below for more information on the use of these buttons.</p> <p>Note</p> <p>If the first line of a SIP phone is empty, Unified CM places the phone into an <i>Unregistered</i> state.</p>

Notes on use of buttons

- **Move Up** and **Move Down**: These buttons are used to shift positional order for the device, based on the checkbox selected next to the *Line* field, these shift either up or down depending on the button clicked. These selected items are shifted one level at a time. Be aware that in certain firmware versions and for certain phone types, for example Cisco 9951, the phone will fail to register or unregister in Unified CM if Line 1 is left empty, even if details for further lines have been specified.
- **Delete Selection**: This button is based on the checkboxes selected next to the *Line* field. Clicking it deletes the selected items.
- **Undo Changes**: This undoes all changes made during the configuration for lines and positions on the device.
- **Select None**: This button deselects all checkboxes currently selected next to the *Line* field.
- **Swap Selected**: Click this button to swap the positional order of the items whose checkboxes are selected next to the *Line* field.
- **Modify**: Click this button to implement all changes made.
- **Cancel**: This cancels out all changes made and returns the user to the *Phone Management* screen.

Step 3 Click the **Modify** button to finalize the transaction.

Add Line

Adding a line is one of the line management features.

Procedure

To add a line:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the device you wish to configure from the displayed list of devices.
- Step 3** Click the **Manage Lines** button under the *Phone Layout* section.

Step 4 Click the **Add** button to configure a number for the selected line position.

Step 5 Select either the *Add Line* radio button or the *Add Clone* radio button as appropriate.

Complete the following fields for the *Add Line* option:

Field	Description
Number	Select from a drop-down list the phone number associated with the line.
Label	Note Text typed in the this field automatically populates the <i>Label ASCII</i> field on the line with the same text. Enter a unique label for the line.
COS	Select from the drop-down list the class of service to allocate to the line. Note When selecting a COS, the corresponding CSS must exist on the Unified CM.

Complete the following fields for the *Add Clone* option:

Field	Description
Selected Line	This drop-down list is used to specify if the line is to be cloned.
Number Clones	Select the relevant number of clones that you would like to make of the line.

Step 6 Click the **Add** button when complete or the **Cancel** button to abort.

Step 7 Click the **Modify** button to finalize the transaction.

Delete Line

Procedure

To delete a line:

Note

- If a voicemail account is tied to a specific extension number on a device associated with the user, and it is the **last instance of that extension number**, the line can only be deleted if the voicemail account for the user is no longer active. For shared lines, where the same extension appears on multiple devices, lines/devices can be removed without affecting the voicemail service **until** there is a single instance of the extension left.
- In certain firmware versions and for certain phone types, for example Cisco 9951, if Line 1 is left empty (either by deleting it or by moving it down), the phone will fail to register or unregister in Unified CM.

Note

From version 8.1.1, Cisco Unified Communications Domain Manager (CUCDM) provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the line(s) being deleted from the phone:

- Logout End User. An end user logged into a device using BVSM Roaming is logged out.

Note

If the end user is logged into the Unified CM extension mobility feature, i.e. BVSM Roaming is not selected, then there is no cascade delete warning, and the end user is **not** logged out of the device. In this instance, the **end user must first log out of the device from the Unified CM** before executing the transaction.

- UC Central. Deactivate and delete UC Central feature if the line is not cloned.
- Voicemail Account. The voicemail account is removed if the end user associated with the phone is the owner of the voicemail account, and the line being deleted is the primary voicemail account number.
- Single Number Reach. Delete the line from destination profiles, if the line is not cloned and is not already shared by another device or mobility profile of the same end user. If it is the last line of the remote destination profile the entire remote destination profile is deleted.

Note

The confirmation popup screen only indicates when a given line is deleted from a remote destination.

- Mobile Identity. Cascade delete the mobile identity associated with the line being deleted.
- Phone Busy Lamp Field references. When deleting a line that is being monitored using a busy lamp field (on the same device or another device), those device busy lamp fields are removed (if the line is neither shared nor cloned).
- Number (Line) Group Lines. The line being deleted is deleted from any associated number (line) groups (if the line is neither shared nor cloned).
- Pickup Group(s). The line being deleted is deleted from any associated pickup groups (if the line is neither shared nor cloned).
- Presence Monitoring. When the line being deleted is monitored for presence, deleting the line automatically removes presence monitoring on the line without any confirmation. The presence service is linked with the end user and not individual lines, and remains enabled.

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the device from which you wish to delete a line. The *Phone Management* screen is displayed.
- Step 3** Click the **Manage Lines** button under the *Phone Layout* section of the screen. The *Line Management* screen is displayed.
- Step 4** Click the **Delete** button adjacent to the line to delete in order to delete the selected line configuration, OR select multiple lines to delete (if required) by selecting the required *Button #* checkboxes and then clicking the **Delete Selection** button. A confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies and you wish to delete the line, proceed with step 8, that is simply click the **Modify** button.

- Step 5** Click the **Delete** or **Delete Selection** button (depending on whether one or more lines is being deleted) on the confirmation popup screen to continue with the delete line/s process. Alternatively click the **Cancel** button to abort the process.

Note

The delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the services being modified as part of the cascade delete action.

- Step 6** Reconfigure the line if required (see *Add Line* above).
- Step 7** Repeat the above steps to delete and/or reconfigure another line (if required).
- Step 8** Click the **Modify** button on the *Line Management* screen when complete to reapply the line configurations, or to delete the line/s (including all dependencies) without reconfiguring - as appropriate.
-

Manage Speed Dials

The Manage Speed Dials section enables you to manage the speed dials for the phone.

View existing speed dials on this screen.

Click the **Add** button to add new speed dial numbers (see [Add Speed Dials on page 814](#)).

Delete individual speed dial numbers (if required) by clicking the **Delete** button next to the speed dial number to delete, or delete all speed dials by clicking the **Delete All** button.

Add Speed Dials

Procedure

The Add Speed Dials section enables you to add speed dials to the phone.

Note

If the *Label* field is not provided and the *Label (ASCII)* field has a valid ASCII value, then the *Label (ASCII)* field's value is used for the *Label* field. If the *Label (ASCII)* field is not a valid ASCII value, then the *Telephone Number* field's value is used for the *Label* field. Similar logic is applied when the *Label (ASCII)* field is not provided.

- Step 1** Complete the required fields (see table below):

Field	Description
Speed Dial Number	The number that you dial on your phone to access the number. This is a mandatory field, select from the drop-down list.
Label	The label (name) of the speed dial number.
Label (ASCII)	An ASCII value for the speed dial number.
Telephone Number	The telephone number or URI dialed by the speed dial short cut. This is a mandatory field. For telephone numbers, valid numbers are 0 - 9, as well as special characters *, #, and +. A URI is in the username@host format, where the host can be an IPv4 address or fully qualified domain name. The username portion of a URI can be a maximum of 47 characters and the full URI a maximum of 254 characters.

- Step 2** Click the **Add** button when complete. The Speed Dial number is added to the phone.
-

Busy Lamp Fields

Busy lamp fields (BLFs) allow a device button to be associated with a specific speed dial or directed call park extension for a user to see the presence status of the line (free or in use). Two types of busy lamp fields are available:

1. Speed Dial busy lamps are like speed dial buttons, but also show the user presence status of the line. The speed dial busy lamps are limited to extension numbers or PSTN in the location of the device.
2. Directed Call Park busy lamps are buttons linked to a specific directed call park extension, but also show the user presence status of the line. The Directed Call Park busy lamps are limited to directed call park numbers added to the location of the device.

Note

- This feature is only available if the phone's button template supports busy lamp buttons.
 - Both types of busy lamp fields are supported in the system, but the two types should not be added to the same device button template. This will lead to unexpected provisioning in the Unified CM .
 - How the busy lamp fields appear on the phone depends on the phone button template and on Unified CM behavior. The *Busy Lamp Field Number* as displayed is the index of the busy lamp field. These are arranged in the same order as they are configured in the Unified CM. For example, the BLF with index 1 would appear on the first BLF button on the phone *according to the button template*, index 2 on the second, and so on. This is also in conjunction with the BLF button type in the button template. For example, if BLF4 is the first directed call park in the template, then in Unified CM this is seen as the fourth directed call park, since that is the index that was passed.
-

The Manage Busy Lamp Fields section on the application GUI enables you to view existing busy lamp fields on this screen and manage the busy lamp fields for the phone.

Click the **Add** button to add new busy lamp fields (see [Add Busy Lamp Fields on page 815](#)).

Delete individual busy lamp fields (if required) by clicking the **Delete** button next to the busy lamp number to delete, or delete all busy lamps (if required) by clicking the **Delete All** button.

To disable a speed dial busy lamp field's *Call Pickup* feature, browse to the device's Busy Lamp Field section, select the relevant busy lamp field and click the *Disable* active text link associated with it.

Add Busy Lamp Fields

The Add Busy Lamp Fields section enables you to add busy lamp fields to the device and/or mobility profile).

If busy lamp fields cannot be added to a device, an error message is displayed and no **Add** button is available:

Message	Comment
"Busy lamp buttons have been disabled for this phone template"	The phone button template associated with the phone has busy lamp fields disabled. For details on the button template associated with the phone type, see <i>Location Administration > Phone Management</i> and Managing the Phone on page 806 .

Message	Comment
"No more busy lamp buttons available (total of x defined for this device)"	Refer to the <i>Max. Number of Busy Lamp Fields</i> entry in the table shown on Phone Type Management on page 39
"The phone button template selected does not support busy lamp buttons"	For details on the button template associated with the phone type, see <i>Location Administration > Phone Management</i> and Managing the Phone on page 806 .

Procedure

Step 1 Complete the required fields. The following fields are available:

Field	Description
Busy Lamp Field Number	The number that this busy lamp field is associated with. This is a mandatory field, and drives the order of appearance of the BLFs on the device - see: Busy Lamp Fields on page 815 .
Label	A label for the busy lamp field.
Label (ASCII)	An ASCII value for the BLF.
Telephone Number	<p>The telephone number associated with the speed dial short cut key.</p> <p>The numbers available on the drop-down list are all numbers from the location assigned to phones or extension mobility profiles, as well as directed call park numbers.</p> <p>The type of extension number that is selected when adding the busy lamp determines the type of BLF (speed dial or directed call park) added to the UC network.</p> <p>This field is disabled if the <i>Destination</i> radio button is selected (see below field).</p>
Destination	<p>A free text destination input field (50 characters maximum). This field can consist of the following characters 0-9, *, #, +, P, p, F, f, C, c or a comma (",").</p> <p>For phones that are running SIP, a SIP URL can be specified in the username@host format, where the host can be an IPv4 address or fully qualified domain name. The username portion of a directory URL can be a maximum of 47 characters and the full URL a maximum of 254 characters. For phones running either SIP or SCCP a telephone number can be specified.</p> <p>This field is disabled if the <i>Telephone Number</i> radio button is selected (see above field). When enabled, the <i>Destination</i> field takes precedence over the <i>Telephone Number</i> field.</p>
Call Pickup	<p>Select the checkbox to enable call pickup for a speed dial BLF.</p> <p>This feature is not relevant for directed call park BLFs.</p>

Note

If the *Label* field is not provided and the *Label (ASCII)* field has a valid ASCII value, then the *Label (ASCII)* field's value is used for the *Label* field. If the *Label (ASCII)* field is not a valid ASCII value, then the *Telephone Number* field's value is used for the *Label* field. Similar logic is applied when the *Label (ASCII)* field is not provided.

Step 2 Click the **Add** button when complete.

Note

- The phone button template associated with the phone or mobility extension must support at least one button type of Speed Dial BLF or Directed Call Park BLF to be able to add a BLF.
-

Manage Service URL

This section enables you to manage the service URLs for the phone.

View existing Service URLs listed on the screen.

Click the **Add** button to add new service URLs for the phone (see [Add Service URLs on page 817](#)).

Delete individual service URLs (if required) by clicking the **Delete** button next to the service URL to delete, or delete all service URLs (if required) by clicking the **Delete All** button.

Add Service URLs

Procedure

The Add service URLs section enables you to add service URLs to the phone.

Note

If the *Label* field is not provided and the *Label (ASCII)* field has a valid ASCII value, then the *Label (ASCII)* field's value is used for the *Label* field. If the *Label (ASCII)* field is not a valid ASCII value, then the *Button Service* field's value is used for the *Label* field. Similar logic is applied when the *Label (ASCII)* field is not provided.

Step 1 Complete the required fields (see table below):

Field	Description
Service URL Number	Only the available Service URL Numbers are available in the drop-down list. If no more Service URL Numbers are available, the add operation fails. In this case, a warning message is displayed next to the drop-down list indicating there are no available slots.
Button Service	Select from available user-level IP Phone Service subscriptions.
Label	A label for the service URL number.
Label (ASCII)	An ASCII value for the service URL number.

Note

The number of available Service URL slots is calculated by the lesser of 1) the number of Service URL slots in the phone button template or 2) the Max. Number of Service URLs specified for the associated Phone Type in the Extension Mobility Profile. In this case, the Phone Type is 7960 SCCP and its associated Max. Number of Service URLs is 10. The Standard 7960 SCCP phone button template has four slots, so the number of available Service URL slots is four. If the Max. Number of Service URLs is updated to a value less than four, this would override the phone button template slots and restrict the number of available Service URL slots that could be assigned.

Step 2 Click the **Add** button when complete. The *Service URL Number* is added to the phone.

Service URLs

See: [Manage Service URL on page 817](#)

Login User

Note

The following must be in place before an end user can be logged in to a phone remotely:

- *BVSMUserRoaming* must be enabled on the provider.
 - The end user must have an Extension Mobility Profile.
 - The end user must either belong to a location not associated with an Extension Mobility Location Group or both the end user and the phone must belong to locations within the same Extension Mobility Location Group.
-

This screen enables you to login users remotely.

Procedure

To login a user remotely:

- Step 1** Select the user you would like to login from the drop-down list.
- Step 2** Click the **Login User** button.
-

The selected user is logged in.

Phone Alerting Names

Note

If you are migrating from a version prior to system release 7.1.1, during the migration process the Alerting Name feature is automatically enabled in the relevant feature group and a default alerting name consisting of the extension number is automatically registered.

Enabling Alerting Names/Alerting Name ASCII

Note

There is no default Alerting Name/Alerting Name ASCII; if the *Alerting Name/Alerting Name ASCII* options are enabled in the Feature Group, and the Alerting Name/Alerting Name ASCII fields are left blank, the values in Unified CM are also blank.

Procedure

To enable the use of alerting names within the system, the feature needs to be enabled within the relevant feature group:

- Step 1** Browse to General Administration > Feature Groups.
- Step 2** Select the relevant *Feature Group* (active text link).
-

- Step 3** Select the *Alerting Name* and *Alerting Name ASCII* options then click the **Modify** button. Alerting Names and Alerting Names ASCII are enabled for the Feature Group.
-

Modifying a Phone's Alerting Name/ Alerting Name ASCII

Note

Before attempting to manage a phone's alerting name, please ensure that Alerting Names have been enabled in the active Feature Group.

Procedure

To modify a phone's Alerting Name:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the required *Phone* (active text link).
- Step 3** Enter the required Alerting Names in the *Alerting Name* and *Alerting Name ASCII* fields.
- Step 4** Click the **Modify** button. The phone's alerting name is updated.
-

Contact Center Agent Lines

The option to set a line as a Contact Center Agent Line will only be available to lines associated with a Feature Group for which this feature has been enabled.

Procedure

To activate a line as a Contact Center Agent Line:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the required *Phone* (active text link).
- Step 3** Select the *Contact Center Agent Line* checkbox in the line's *Common Line Settings* section.
- Step 4** Click the **Modify** button.
-

Replace a Phone

Procedure

To replace a phone and retain all of its settings:

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the required *Phone* (active text link).
- Step 3** Click the **Replace Phone** button.
- Step 4** From the list of available phones, click the **Select this Phone** button of the phone that will replace the current phone.
-

Note

- This function is disruptive to end users making phone calls.
 - Only phones of the same type can be used to replace the current phone with.
-

Unregistering / Deleting a Phone

Note

- If a voicemail account is tied to a specific extension number on a device associated with the user, and it is the **last instance of that extension number**, the device can only be unregistered/deleted if the voicemail account for the user is no longer active. For shared lines, where the same extension appears on multiple devices, lines/devices can be removed without affecting the voicemail service **until** there is a single instance of the extension left.
 - When a phone is unregistered, it is automatically placed into the location's default device pool.
-

Procedure

Unregistering a phone removes the number from it, thus the phone can no longer make or receive calls. However, the phone still maintains its IP Address in the location.

Note

From version 8.1.0, Cisco Unified Communications Domain Manager (CUCDM) automatically removes/clears the following elements associated with a phone during the unregistering a phone process:

- Speed dials
- Busy lamp fields
- Service URL's
- IP phone service subscriptions

In addition to this, from version 8.1.1, CUCDM provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the registered phone being unregistered:

- Phone disassociate (refer to [Associate/Unassociate \(or Delete\) Device with/from User](#) on page 852 for details on these dependencies)
- Delete phone lines (refer to [Manage Lines](#) on page 810 for details on these dependencies)

Note

Certain phone types, for example IMS-integrated Mobile (Basic), Cisco Unified Mobile Communicator, CTI Remote Device, and Carrier-integrated Mobile are tagged with a mandatory *Owner User ID* flag, and must **always** be associated with a user. For this reason, these phone types can not be unregistered in the normal way, and the **Unregister** button on the relevant *Phone Management* screen is replaced with a **Delete** button. In addition to the above dependencies, the following actions are taken during the delete process of this type of phone.

- Phone is moved from the location
- Phone is deleted from phone inventory

- Step 1** Browse to *Location Administration > Phone Management*.
- Step 2** Select the *Device Name* (active text link) of the phone you want to unregister/delete (as applicable).
- Step 3** Click the **Unregister** (or **Delete**) button (as appropriate) at the bottom-right of the screen. A confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies, the phone is immediately unregistered (or deleted) as applicable.

Step 4

Click the **Unregister** or **Delete** button (as appropriate) button on the confirmation popup screen to continue with the unregistering/deleting a phone process. CUCDM removes/clears the relevant associations and unregisters (or deletes) the phone. Alternatively click the **Cancel** button to abort the process.

Note

The unregister/delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

Refer to the Self Care Guide for detailed information about the following:

- Managing Phone Details
- Managing Line Details
- Managing Phone Features
- Managing Line Features
- Managing Busy Lamp Fields
- Managing Speed Dials

Location Administration Tools

An administrator with the **LocationTools** permission (as set in the administrator's Access Profile) will have access to and be able to execute *Location Administration > Administration Tools*.

Location Administration Tools allow for the automation of multi-step processes, such as resetting all phones in a location. The following location administration tools are available:

Operations Tool	Description	Remarks
Location Level		
Logout all roaming end users of a location from all phones.	Logs out all roaming end users in a location from their phones.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the <i>tool's</i> active text link, click the Submit button once you are sure you would like to proceed.</p>
Reset all phones at a location	Resets all phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the <i>tool's</i> active text link, click the Submit button once you are sure you would like to proceed.</p>

Operations Tool	Description	Remarks
Set Location Codecs	Sets the Customer Codecs for the <i>Intra-Location Max Audio Bit Rate</i> and the <i>Inter-Location Max Audio Bit Rate</i> .	Use the drop-down lists to select the <i>Intra-Location Max Audio Bit Rate</i> and the <i>Inter-Location Max Audio Bit Rate</i> then click the Submit button.
Voicemail Caller Input Extension Search	<p>Caller input settings define actions that Cisco Unity Connection takes in response to the phone keypad keys that are pressed by callers during a user greeting.</p> <p><i>The Voicemail Caller Input Extension Search</i> feature allows an administrator to replace existing extensions that are associated with specific keys.</p>	Enter the new extension in the <i>Replace with Extension</i> field and then click the Replace All button.

See the table under [Operations Tools on page 515](#) for a list of available operations tools.

Unmanaged Locations

The functionality allows a location to be added as an unmanaged location in the system. An unmanaged location supports only PBXs that are unmanaged. They don't require any phone management, mobility management, CTI device management or analog line management in the system.

When adding an unmanaged location, we need to configure an unmanaged PBX and add a hardware group having usage *Add Locations-Unmanaged*.

Note

The same unmanaged PBX and hardware group can be used for all unmanaged locations.

Adding an Unmanaged PBX

To add an Unmanaged PBX, navigate to *Network > PBX Devices*, click the **Add** button, select the product *Unmanaged PBX* and then click the **Add** button.

Configure the following settings listed on the page then click the **Add** button:

- Host Name
- Description
- **Country:** Select from the drop-down list.
- Email Address
- **IPPBX CPID:** Select from the drop-down list, select AUTO to allocate the next available one.
- **IPPBX CID:** Select from the drop-down list, select AUTO to allocate the next available one.

Adding a Hardware Group for Unmanaged Locations

To add a *Hardware Group*, which can be used for adding an *Unmanaged Location*, browse to *Network > Hardware Groups* and click the **Add** button. Configure *Limit Usage for this Hardware Group* setting to *Add Locations - Unmanaged* and click the **Next** button.

The next page lists the Available Transit Switches and Unmanaged PBXs available for selection in the Hardware Group. Select the appropriate servers and click the **Add** button.

Adding an Unmanaged Location

To add an Unmanaged Location, browse to *General Administration > Locations* and click the **Add** button. Select *Unmanaged Location* as the Location Type and click the **Next** button. The *Hardware Group* drop-down list lists the hardware group having usage as *Add Locations - Unmanaged* for unmanaged locations.

Location Administration for Unmanaged Locations

Location Administration Modules: *Hunt Groups, Number Groups, Pickup Groups, Phone Inventory, Phone Registration, Phone Management, Analog Line Mgt and MoH Tracks*; Also *CTI Devices Management, Call Park and Directed Call Park* pages under *Location Administration > Telephony* are not relevant to unmanaged locations and therefore display a message *Not Available for Unmanaged Locations*.

Allocated Connectivity for the Location

The Unmanaged location is generally connected to the architecture via a Session Border Controller (SBC) or a Legacy Gateway. The choice and management of this connectivity is done via the *Location Administration > Telephony > SIP Devices OR Legacy Gateways* links.

Resource Management

The system provides the means to manage inventory of different types. Resources / Inventory can be managed at some or all hierarchy levels.

In order to allow you to manage any type of Resource, it needs to be granted from a higher level in the hierarchy (aka parent) to the level you want to use it in.

The following hierarchy levels are supported in the system for management and use of resources (from the highest to the lowest):

Hierarchy levels

1. Provider
2. Reseller
3. Building
4. Customer
5. Division
6. Location
7. User

The Resources in the system can be of a different nature:

- Physical and Network Resources, for example Phones, IP Addresses
- Services, for example Voicemail, Conference
- General/Supporting data, for example Site codes)

The table below is a guide to resources and the hierarchy level at which you can manage them:

Resource	Type	Managed at level:	Used at level
E164 Numbers (DDIs / DIDs / FNN)	Physical	1 and 6	6
Billing Codes	General	1 to 7	2 to 7
Managed IP Subnets	Physical	1 and 4	6
Site Codes	General	4	6
Voicemail	Service	4 and 6	7
Auto Attendant	Service	4 and 6	5
Console	Service	4 and 6	6 and 7
Media	Service	4 and 6	6 and 7
Phones	Physical	1, 2, 4 and 5	6
Contact Center	Service		
Analog lines	Physical		6
MoH	Service	5	7
Internal Numbers (extensions)	Physical	6	7
External Numbers	Physical	6	7

Managing Available Internal Numbers

An administrator may be required to manage add or remove available extensions within a location. Without available extensions, phone numbers are not available in the location.

Usually when a location is created, the range of applicable extensions is made available as part of the creation process.

However, in case of changes or if the required extensions are not available in the location, the administrator can manage at the location level.

Additionally, internal numbers can be managed in ranges as described below.

There are several ways to find an extension, the easiest is via the *Internal Extensions* menu option at the location level (*Location Administration > Internal Extensions*).

Procedure

Find Internal Numbers

To find an extension via the Internal Extensions menu:

Step 1 Browse to *Location Administration > Internal Numbers*.

Note

The resulting screen shows the first 50 internal numbers provisioned in the location that are available for registration.

Step 2 To find a specific extension or reduce the list displayed, select the required search criteria from the *Search* drop-down list, then type information in the field provided and click the **Search** button. The following search criteria are available:

- **Number Ends with** - all or last few digits of the extension, for example 5 = internal extension ending with 5
- **Number Starts with** - all or first few digits of the extension, for example 23 = internal extension starting with 23

- **Reserved** - any part of the number for reserved extensions
- **Available** - extensions allowed in the location

The following information and actions are available on this page:

Field	Description	Remarks
Internal Number	Internal Extension	The system shows the action that can be done on the number and from the action you need to deduce the number status. This is a mandatory field.
Associated PSTN Number	DDI linked to the Extension.	-
Used By	The entity the number is allocated to.	-
Device Groups	The device groups related to the range.	-
CLI Groups	Internal numbers can be associated with a CLI Group (Calling Line Identification)	<p>The CLI Group is managed at Customer and Location levels, where the number can be removed from the CLI Group.</p> <p>Internal numbers cannot be deleted if they belong to a CLI group as either a member of the group or its internal configuration extension number. The delete transaction fails when the number is used by a CLI Group.</p>

Procedure

Managing Internal Number Ranges Allocated to the Location

To manage extension ranges allocated to a location:

- Step 1** Browse to *Location Administration > Internal Numbers*.
- Step 2** Click the **Extension Range Management** button.
- Step 3** To delete a range, click the **Delete** button adjacent to the range that you would like to delete.

or

To allocate a range, select the *Add Extension Range* active text link adjacent to the required number range.

Procedure

Managing Internal Number Ranges

To manage extension ranges:

- Step 1** Browse to *Location Administration > Internal Numbers*.

Step 2 Click the **Extension Range Management** button.

Extensions are managed using ranges:

- Option 1

Enter the start extension and the end extension number, then click either the **Add Extension Range** or **Delete Extension Range** button.

or

- Option 2

Enter the required extension range, for example, 0000-0100, 0200-0299 and so on, then click the **Add Extension Range** or **Delete Extension Range** button.

Note

Extensions (Internal Numbers) can be managed via the bulk loaders.

External numbers

E164 numbers (DDIs / DIDs / FNNs) are a limited resource. They are the cornerstone of the PSTN telephony system. As such they are managed by the Service Provider (SP) and allocated at that level, to the location.

DDI numbers are already allocated to your Location by the Service Provider. If DDI numbers are not present, or you have used all your numbers, then you need to request additional numbers from your Service Provider.

At the location level you can only use E164 numbers (External Numbers) which have been allocated. To manage the E164 numbers in the location you need to follow the process.

Find External Numbers

There are several ways to find an external number:

- Via the External Extensions menu option at the location level (*Location Administration > External Numbers*)

Procedure

To find an external number via the *External Numbers* menu:

Step 1 Browse to *Location Administration > External Numbers*.

Step 2 To find a specific external number or reduce the list you can use the following search criteria before selecting *Search*:

- **Country Numbers:** Including specific ISO country code
 - **National Area Code:** Any number of digits from the start (or the full) national area code without any leading digits. For example:
 - 2 returns numbers allocated to the location with 207 and 208 area codes
 - 16 returns numbers allocated to the location of 1638 and 1635 area codes but not 118
 - **Local Number:** Any number digits from the start of the PSTN number.
-

The following information and actions are available from the list of external numbers:

Country	ISO Country Code.	-
National Area Code	Area Code prefix for the PSTN number.	-
Local Number	The PSTN Number.	-
Internal Extension	The internal number associated with the PSTN number.	If no extension is associated with the PSTN number - Not Associated
Breakout	The current breakout point of the number, for example, Central.	-
Device Group (Tenant)	The device group currently utilizing this number.	-
<i>CLI Group</i>	E164 numbers can be associated with a CLI Group (Calling Line Identification).	<p>The CLI Group is managed at Customer and Location levels, where the number can be removed from the CLI Group.</p> <p>The user is not allowed to disassociate or associate an external number which is used by a CLI Group - either as a member of selected extensions or as the group External configuration E164 number. In case associate or disassociate is attempted on a number which is in use by CLI groups the requested transaction fails.</p>

See also:

- [External numbers on page 826.](#)
- [Managing Available Internal Numbers on page 824.](#)

External Numbers Range Management

E164 numbers are a limited resource and form the cornerstone of the PSTN telephony system. The PSTN to Extn Range Mapping screen is divided into three sections, *Details*, *Map a PSTN Range to multiple extensions* and *Map a PSTN Range to a single extension*.

Usually, there are multiple PSTN numbers in a location. Therefore the system supports the management of a range of numbers.

If you are managing a location that has the AssociateFNNinRanges preference enabled, you need to specify the range size when managing associated FNNs. The AssociateFNNinRanges preference can be enabled by browsing to location preferences and selecting the enable checkbox for this preference. When enabled, FNNs associated at the location level are associated in ranges. You are able to specify the size of each range when you are associating FNNs.

Note

If any of the extensions being associated/disassociated are currently configured on a device (phone, extension mobility profile, CTI, or analog), you must run the Ops tool *Update All Phone/Extension Mobility/CTI Line Masks At Location* after the associate/disassociate task to update the relevant line mask/s at the location - see [Operations Tools on page 950](#) if required.

Procedure

To associate a range of external numbers:

Step 1 Browse to *External Numbers* from the *Location Administration* menu.

Note

This functionality is also available for Location Management, Conference services, Voicemail services and Buildings

Step 2 Click the **Associate Range** button.

Step 3 Configure the fields as required, the following three fields are displayed: *Country* (read only), *National Code* (read only), *Range Size* (select from drop-down list - 10000, 1000, 100, 10 or 1).

Step 4 Click the **Next** button when complete.

Step 5 Select the PSTN Template (if required) from the drop-down list in the *Details* section. The *LocalGW* option must be selected if the *Location Local Gateways* checkbox is selected in the associated hardware group (see [View and Delete a Hardware Group on page 147](#)). If you are unsure what template to select, please contact your dedicated system account manager.

Note

Depending on whether you would like to work with multiple or single extensions, select either the *Map a PSTN Range to multiple extensions* or *Map a PSTN Range to a single extension* radio button (section).

Step 6 Select the required range of PSTN number ranges and extension numbers from the drop-down lists, the *Keep Current Primary E164* or *Assign New Primary E164* radio button as required, and click the **Submit** button. See table below for field descriptions.

Field	Description	Remarks
PSTN Number Range	The PSTN number range to associate.	Select from the drop-down list. Default = first range in list. The list displays the PSTN number ranges of the chosen area code which are not yet associated with an internal extension.
Extension Numbers	The internal number or number range to associate.	Select from the drop-down list. Default = first number or number range in list. The list displays the internal extension number/s that are available in the location and not yet associated with any PSTN number.
Keep Current Primary E164	Select this checkbox if you would like to use the current Primary E164.	Only available if mapping to a single extension.
Assign New Primary E164	Select this checkbox if you would like to specify a new Primary E164.	Select the new number from the adjacent drop-down list. Only available if mapping to a single extension.

See also:

- Managing Internal Number Ranges at [Managing Available Internal Numbers on page 824](#).

Disassociating Range of External Numbers

Procedure

To disassociate a Range of External Numbers:

- Step 1** Browse to *Location Administration > External Numbers*.
- Step 2** Click the **Disassociate Range** button.
- Step 3** Select the required PSTN Number Range you want to disassociate from the drop-down list.
- Step 4** Click the **Remove Association** button.

Note

The system does not allow disassociation of numbers in use, for example numbers which are allocated to users or phones, numbers used as pilot, and so on.

Available fields include:

Field	Description	Remarks
Range - PSTN Number Range	The PSTN number range set from which extension mapping must be removed.	<p>Select from the drop-down list.</p> <p>Default = first number range in list.</p> <p>The list displays the PSTN number ranges of the chosen area code which are associated with an internal extension.</p>

Managing Primary E164 Numbers

This page enables you to select either Primary PSTN or Extensions. If you select Primary PSTN, the extensions mapped to that number are listed. The current Primary E164 is also displayed. If you select Extensions, the numbers mapped to that extension are listed for selection, the current Primary E164 is also indicated.

Note

- When mapping on a one to one basis, there is no option to select a prime number as the number is automatically the prime number.
- All associations must have a prime number.
- When working with associations, one can change the prime number or keep the current (the current is displayed if a number already has one).
- Prime E164 numbers can be managed from multiple menu locations such as *Voicemail Services*, *Conference Services*, *Location Management* and *Buildings*.

Procedure

To manage Primary E164 Numbers:

Step 1 Browse to *Location Administration > External Numbers*.

Note

Prime E164 numbers can also be managed from menu locations such as *Voicemail Services*, *Conference Services* and *Buildings*.

Step 2 Click the **Manage Primary E164 Number** button.

Step 3 Select the required *National Area Codes* then click the **Next** button.

Note

In some countries, area codes are not in use, so the system also supports a *None* value.

Step 4 Select either the *Primary PSTN* or *Extension Number* radio button then select the relevant *Primary PSTN* or *Extension Number* from the drop-down list.

Step 5 Click the **Next** button.

Step 6 The current primary number is displayed along with a drop-down list of available Primary E164 numbers. Select the new Primary E164 number from the drop-down list then click the **Submit** button.

The Primary E164 number is updated.

Phone Inventory

Phones are one of the key resource elements managed by the system. Phones can be created at the Provider, Reseller, Customer, Division or Location administration level, depending on the configuration of the relevant administrator's access profile settings. The system tracks the Phone inventory throughout this process and provides both inventory tracking as well as feature management for each phone. At location level, the administrator can view the phones in the location inventory and perform limited functions.

There are several ways to find a phone:

- Via the Phone Inventory menu option at the location level (*Location Administration > Phone Inventory*).
- Via the Phone Inventory menu option in the Resources menu (*Resources > Phone Inventory*).
- Via Quick Search

Procedure

Find Phone via the Inventory menu

Step 1 Browse to *Resources or Location Administration > Phone Inventory*.

Step 2 To find a specific Phone or reduce the list displayed, you can use the following search criteria:

- *Device Name starts with*: One or more characters from the start of the phone Device Name
 - *Unregistered*: Phones which are allocated to the location but are not yet registered
 - *Registered*: Phones which are registered in the location
 - *Device name ends with*: One or more characters at the end phone Device Name
 - *Phone Type*: The list of phones by phone type (need the full phone type if criteria is filled)
-

Note

Search of Device names is not case sensitive.

The following information and actions are available from the list of phones:

Field	Description	Remarks
Phone Type	Phone type	The type of phone.
Device Name	Device Name	This is an active text link. Selecting the active text link presents more information regarding the phone.
Registered	Y or N	This is an active text link. Y = registered. Click the Y (active text link) to access the <i>Phone Management</i> screen in order to unregister the phone if required.
First Line Ext / Label	Information from the 1st line of the phone if registered.	Label is shown if it is not set to default. When the phone is not registered, no information is presented.
Reseller	Phone reseller	-
Customer	Phone customer	-
Division	Phone division	-
Location	Phone location	-
Device Group (Tenant)	Phones device group	-
Service Status	In Service / Out of Service / Partially out of service (limited calling options)	<p>This is an active text link. <i>In Service</i> - phone available for service. Selecting active text link takes the phone out of service.</p> <p><i>Out of Service</i> - phone not available for service. Selecting the active text link places the phone <i>In Service</i>.</p> <p><i>Partially out of service (limited calling options)</i> - if the first line of the phone is suspended (using Operations Tool <i>Suspend All Phones At Location Out of Service/First Phone Line Only</i> checkbox), then the first line of the device is not available for service and cannot be used currently. Selecting the active text link puts the phone back into <i>In Service</i> mode.</p> <p>Note</p> <p>This option is only available after running the Operations Tool <i>Suspend All Phones At Location Out of Service</i>, and selecting the <i>First Phone Line Only</i> checkbox).</p>

Viewing and Modifying a Phone in the Inventory

Note

Phones can be added to the system at any level and moved to the same or lower hierarchy level. The phone can only be provisioned and registered at a location. Therefore, you will need to move it into the location as required. Similarly, when the need to clear the phone from the system arises, you will need to move the phone out of the location and back into the provider level in order to delete it.

Procedure

To view or modify a phone

- Step 1** Select the *Phone Inventory* option from either *Resources* or *Location Administration* (depending on your log in access level).
- Step 2** Select the *Device Name* (active text link) that you would like to view, or to modify (only if the device is unregistered)
- Step 3** View the displayed values (note that fields may differ depending on the status of the phone as well as the log in access level). The following fields are displayed on the first screen, these include:

Field	Details
Device Name	The device name. This field is for information purposes only and cannot be modified here.
Phone Type	Phone Type. This field is for information purposes only and cannot be modified here.
Configuration Profile	Indication that this is not a real phone. This field is for information purposes only and cannot be modified here.
Button Template Name	Phone button template. This field is for information purposes only and cannot be modified here.

- Step 4** Click the **Next** button (to modify/move the unregistered phone) .

Take note of the following rules for moving phones:

Phone allocated to	Can be moved to
Provider	Any level in the hierarchy below the provider.
Reseller	<ul style="list-style-type: none"> • Back to the provider - Unassigned • To any entity which belongs to this reseller, for instance the customer, division, location of this reseller.
Customer	<ul style="list-style-type: none"> • Back to the provider - Unassigned • Back to the reseller. • To any entity which belongs to this customer, for instance the division, location of this customer.
Division	<ul style="list-style-type: none"> • Back to the provider - Unassigned • Back to the reseller • Back to the customer • To any location which belongs to this division

Phone allocated to	Can be moved to
Location	<ul style="list-style-type: none"> • Back to the provider - Unassigned • Back to the reseller • Back to the customer • Back to the division

Step 5 Modify the required fields. The following additional field is available on the second screen:

Field	Details
Select a Move Target	Select a location, or any other hierarchy, where you would like to move the phone. This is selected from the drop-down list. Default=Unassigned. If unassigned, the phone is automatically added at the Provider level, from where it must be manually assigned to lower administration levels by a Provider or System Administrator as required.

Step 6 Click the **Next** button to select a subnet (if applicable).

Step 7 Review the information on this screen. Available fields include:

Field	Details
Device Name	The device name. This field is for information purposes only and cannot be modified here.
Select Subnet	If applicable, select the required subnet from the drop-down list. Only relevant to the location administration level. Note that the <i>Don't manage phone subnet</i> option is only applicable to mobile devices such as the Nokia S60 and Cisco dual mode devices.

Step 8 Click the **Move Phone** or **Add Phone** button (as appropriate). The phone information is updated with the relevant changes.

Procedure

Deleting a Phone from the Inventory

To delete a phone:

Note

- Phones can be deleted at the reseller, customer, division, or location administrator levels depending on the configuration of the relevant administrator's access profile settings. Higher administrator levels can delete phones at the same or lower administrator level.
- Only provider and system administrators can delete a phone which is currently unassigned.
- Only phones which are not registered on location level can be deleted.

Step 1 Select the *Phone Inventory* option from either *Resources* or *Local Administration* (as applicable).

Step 2 Select the *Device Name* (active text link) that you would like to delete.

Step 3 Click the **Delete** button. The phone is removed from the inventory.

Adding a Phone to the Phone Inventory

Note

- Adding a phone can be performed at the Provider, Reseller, Customer, Division or Location administration level, depending on the configuration of the relevant administrator's access profile settings.
 - Regardless of the level in the hierarchy you are when adding a phone, it is added at the Service Provider level unless it has been assigned to a specific hierarchy level.
-

Procedure

- Step 1** Browse to *Resources or Location Administration > Phone Inventory*.
- Step 2** Select the relevant *Service Provider* (if applicable). The *Phone Inventory* screen is displayed.
- Step 3** Click the **Add Phone** button to add a phone to the inventory.
- Step 4** Enter the required information in the relevant fields (see table below for a list and description of each field).
- Step 5** Click the **Next** button to go to the next screen (only applicable if adding a phone at location level).

Field	Description	Remarks
Select a Move target	Specifies the administrator user hierarchy level that has access to the added phone.	Select from the drop-down list. Default = Unassigned. If unassigned, the phone is automatically added at the Provider level, where it must be manually assigned to lower administration levels by a Provider or System Administrator as required.

Field	Description	Remarks
Phone Type	New phone type.	<p>The first <i>Phone Type</i> field is a searchable field used to refine the search. For example if searching for a Nokia phone, type Nokia in the first <i>Phone Type</i> (search) field. The adjacent drop-down list automatically displays the phone that matches the search criteria, and the user can then navigate up and down the list from that point to select the required phone type. Select the required <i>Phone Type</i> from the drop-down list. If the phone type supports the "Use Alternate Site CSS" feature, then the phone's CSS name setting on the Unified CM is modified when the phone is added and registered.</p> <p>Note</p> <p>Certain phone types must be associated with an end-user, and therefore have a mandatory owner user ID field. These phone types, which include, IMS-integrated Mobile (Basic), Carrier-integrated Mobile, and CTI Remote Device, have a modified provisioning workflow, whereby the CUCDM combines the Add (AddPhone), Move (MacToLocation), Register (RegisterPhone), and Associate (AssociateUserPhone) transactions into one step. See Add, Move, Register and Associate a Phone - One Step Process on page 837 for this updated process.</p> <p>Default = 1st value in list.</p>

Field	Description	Remarks
Device Name / Enter the MAC address of the phone	The new phone's device name (MAC address).	<p>Note</p> <p>The field name displayed is dependent on the phone type selected (see above field).</p> <p>The device name (MAC address) is validated according to the device name format for the device's phone type (see Phone Type Management on page 39).</p> <p>Only capital letters A to F and numbers 0 to 9 (12 maximum) can be entered in the MAC address field. Any characters (50 maximum) can be entered in the Device Name field.</p> <p>This is a mandatory field.</p>
Full Device Name	This is the full device name the system uses to manage the device.	This field is automatically updated by the system.
Configuration Profile	This checkbox is used to mark the phone as a dummy phone to be replaced later as part of phone based registration of an actual phone.	<p>Note</p> <ul style="list-style-type: none"> • This field is only available for MAC-based devices as the location of these devices is typically unknown and they are auto-moved to the location as they are plugged in. In practice, this setting is only used by devices that can use XML phones services, and so on. • If the item selected is a device and not a phone, the checkbox is selected but hidden. If the item selected is a phone, then the checkbox is displayed but not selected (unchecked) by default. <p>See Phone Based Registration on-page 788 if required.</p>

Field	Description	Remarks
Select Subnet	Allows you to select the required subnet when moving a phone.	Select from the drop-down list. Only relevant to the location administration level. Note The <i>Don't manage phone subnet</i> option is only applicable to mobile devices such as the Nokia S60 and Cisco dual mode devices.
Button Template Name	Specifies the button template in use by the phone.	Only relevant to the location administration level. Button templates are determined by the selected Phone Type.

Step 6 Click the **Add Phone** button when complete.

Move Phone Automatically

Alternatively, utilize the *Auto Move* functionality to move phones into the correct location.

There are a few prerequisites that must be in place before the Auto Move functionality can be used. These must be completed as part of the deployment by the system's deployment team based on the defined business requirements. Please confirm with the system administrator that the following is in place:

- The system's Auto Inventory and Move Phones setup is configured correctly
- The system's autoreg (syslog) is setup and configured

Procedure

To trigger phone moves automatically:

- Step 1** Add the phone device name to the system at the provider level.
- Step 2** Enable the *AutoMoveCustomer* preference for the customer.
- Step 3** Enable the *AutoMoveLocation* preference for the required location.
- Step 4** Plug the phone into the network. The system identifies that a new phone was connected to one of its subnets and moves the phone to the location which this subnet belongs to.

Note

Normally this process is used for the bulk load of phones. The phones (Device Names) are added to the system and can then be distributed without the need to pre-confirm what device names are allocated to what location.

Add, Move, Register and Associate a Phone - One Step Process

Procedure

To add, move, register and associate a phone type:

Step 1 Browse to *Location Administration > Phone Inventory*. The *Phone Inventory* screen is displayed.

Step 2 Click the **Add Phone** button.

Step 3 Enter the required fields on the Phone Inventory screen. The following fields are available:

Field	Description	Remarks
Select a Move target	Select the required move location for the phone from the drop-down list.	This provides the required reseller, customer, division and location hierarchy.
Phone Type	Select the required type of phone by using the drop-down lists.	The first drop-down list is a text field, which is used to refine the search. For example if searching for an IMS phone, type <i>IMS</i> in the first <i>Phone Type</i> field. The adjacent drop-down list displays all available IMS phone types.
Device Name/Enter the MAC address of the phone	Enter an appropriate device name or MAC address.	For example <i>IMS TEST</i> . The text entered in this field automatically populates the <i>Full Device Name</i> field below.
Full Device Name	The full device name.	This field is populated with the same text entered in the <i>Device Name/Enter the MAC address of the phone</i> field above.

Step 4 Click the **Next** button to continue with the process.

Step 5 Enter the required fields on the next screen. The following fields are available:

Field	Description	Remarks
Select Subnet	Select from the drop-down list the required subnet to use when moving a phone.	Only relevant to the location administration level. Note The <i>Don't manage phone subnet</i> option is only applicable to mobile devices such as the Nokia S60 and Cisco dual mode devices.
Button Template Name	Select the required button template name from the drop-down list.	To make sure that the correct phone button templates are displayed, import the latest phone button templates from Unified CM as described in Importing/Refreshing CCM Items on page 87 .

Step 6 Click the **Continue to Register Phone** button to continue with the process. The *Phone Registration* screen is displayed.

Step 7 Enter the required *Phone Features* fields. The following fields are available:

Field	Description	Remarks
Description	A description of the phone.	-

Field	Description	Remarks
SIP Profile	Select from the drop-down list.	Only available for SIP type phones.
Button Template Name	Select from the drop-down list.	-
Phone Security Profile	Select from the drop-down list.	-
Media Services	Select from the drop-down list.	-
<i>Device Group</i>	Select from the drop-down list.	-
<i>Select Phone Feature Group</i>	Select from the drop-down list.	-
<i>Device Calling Search Space</i>	Select from the drop-down list.	-

Step 8 Click the **Next** button to continue with the phone registration process.

Step 9 Enter the required fields, the following fields are available :

Field	Description	Remarks
Device Use	Select from the drop-down list.	Phone or Fax.
SRST	Select checkbox if this is an SRST phone.	Available only for SRST phones.
SRST Reference	Select the SRST Reference for the SRST phone from the drop-down list.	-
Device Pools	Select the required device pool from the drop-down list.	All device pools available at the specific location are displayed in the drop-down list.
Number Details	Select from the drop-down list.	-
User Details	Select a user to associate with the phone from the <i>Associated user</i> drop-down list.	This is a mandatory field for phone types that have the <i>Owner Username Required</i> checkbox selected.

Step 10 Click the **Next** button to continue with the phone registration process.

Step 11 Click the **Register** button to complete the phone registration process.

Managing Users

This section describes how an administrator is able to manage end users within the system. This includes adding new users, modifying settings of existing users and deleting users.

Note

- It is important to refer to the *LDAP Integration Guide*, specifically in relation to the limitations and prerequisites of user management (adding, modifying and deleting) in a CUCDM-LDAP integrated system environment.
- Every user has to be associated with a specific location.

Find a User

There are two methods available to find a specific user:

- Via the *User menu* option at the Location Administration level (*Location*) - see "Location Administration User Search" / step 1 below.

- Via *Quick Search* - see *Location Administration User Search* / step 2 below.

Procedure

Location Administration User Search

- Step 1** Select the *User* option from the *Location Administration* menu. The screen shows, by default, the first 50 users in that location.
- Step 2** To find a specific user, or reduce the number of users displayed, select the search criteria from the *Search by* pull-down selection list, type as many characters as you know in the field provided and then click the **Search** button.

The following search criteria are available:

Username - all or part of the username (e.g. "ab" search returns all users who have the letters "ab" in their username).

Surname (last name) - the user last name or part of it (e.g. "smi" search returns all users who have the letters "smi" in their last name).

Note: The search string is not case-sensitive.

The following information is shown for each user in the User List:

Field	Description	Remarks
Username	Active text link	When used (selected) this opens a screen with the user details allowing you to manage this specific user
Name	Concatenation of the user First Name and Last Name.	-
Role	User role in the platform.	User can only have one role. The user role defines what "type" of user they are and what sort of functions they can perform in the system. For example: <ul style="list-style-type: none"> • End User • Location Administrator
Device Group (Tenant)	Name of Device group associated with the phone.	If none, N/A is displayed.
Associated Device(s):First Ext	List of devices (phones/analog lines) associated with this user. Also displays the first extension number for the device (if applicable).	List presented in the structure of Device Name:EXT
Voicemail	Active text link: <ul style="list-style-type: none"> • Add • N/A • Y 	When used opens the screen to manage (or add) a VM box for the user. <p>Note</p> <p>VM is only added to a user who has a phone number (Associated Device or Extension Mobility profile).</p>

Field	Description	Remarks
Conferencing	Active text link: <ul style="list-style-type: none"> Add N/A Y 	-
Presence	Active text link: <ul style="list-style-type: none"> Add N/A Y 	Click <i>Add</i> , to open the <i>Presence Configuration</i> screen. From here, you can select checkboxes to; <i>enable</i> the Presence feature for the user, as well as to <i>monitor</i> the relevant device extension.
Extension Mobility	Active text link: <ul style="list-style-type: none"> Add Extension Mobility Profile details 	Click <i>Add</i> to open the <i>Add Extension Mobility Profile</i> screen. This screen is used to add an extension mobility profile for the user. If the user already has an extension mobility profile, Ext(s) and their status is shown.

Delete a User

From version 8.1.1, Cisco Unified Communications Domain Manager (CUCDM) provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the end user account:

- The personal address book of the end user is removed.

Note

This action is not displayed in the confirmation popup screen.

- The extension mobility profile of the end user is removed - if configured (see [Extension Mobility Profiles on page 854](#) for details).
- Associated phones. Any phones associated to this end user are unassociated unless they are phones that require an owner ID or are dual mode phones (see [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#) for details). Phones associated to this end user that require an owner ID or are dual mode phones are deleted.
- Analog Lines. All analog lines associated to this end user are unassociated-associated (see [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#) for details).
- Conference. All conference services for this end user are removed.
- Presence. Presence licenses tied to this user are removed

Procedure

To delete a user account:

Note

If the User has a Voicemail account that is referenced in the Caller Input of another user, the reference must first be removed before the user can be deleted.

Step 1 Select the *Username* (active text link) of the user you want to delete on the *End User Management* screen.

Step 2 Click the **Delete** button (located at the bottom-right of the screen). A confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies, the user is immediately deleted.

Step 3 Review the associated dependencies and click the **Delete** button on the confirmation popup screen to continue with the delete process. The system de-provisions the user in the platform and clears the user from its database. Alternatively, click the **Cancel** button to abort the process.

Note

The delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

Note

To move a user, delete the user account and then recreate the account in the new location.

Add an End User

When you create an end user from the *Location Administration* menu, a user account with an end user role is added to the system's database and linked to the location in which the administrator is currently operating in.

To add an end user account to a different location, you must login to an account linked to that location with location administrator privileges. Alternatively, if you are logged in with higher level privileges (e.g. Customer Administrator), you could use the *Quick Search* option or the list of locations via the *General Administration > Locations* menu.

The User Management page displays the existing user accounts for the current location.

Procedure

To add a new end user:

Step 1 Click the **Add** button at the top of the user list.

Step 2 Enter the user's details. The fields available in this section of the screen are to do with basic user information. The following fields are available:

Field	Description	Remarks
Username	The id of the user	<p>This is a mandatory field.</p> <p>Must be unique across the platform.</p> <p>Best Practice: Consider user name convention see above.</p> <p>Note</p> <p>If a user group is associated with the user (only available from system version 8.0), the specified user group is automatically displayed adjacent to the username field to create a unique username, for example; username@usergroup. The special character '@' is allowed in a username.</p> <p>See also the <i>UsernameValidation</i> setting at Provider Preference and Settings on page 937</p>
Security Profile	The security profile related to the user.	Select the required security profile (if required) from the drop-down list. Options include security profiles that have been configured for your system as well as the <i>None</i> and <i>Default</i> options.
Password	Initial password for user login into the system.	This is a mandatory field.
Role	User role in the platform.	<p>Select from drop-down list. Default = End User.</p> <p>User can only have one role. The user role defines what type of user they are and what sort of functions they can perform in the system.</p> <p>For example:</p> <ul style="list-style-type: none"> • End User • Location Administrator
Title	Title of user.	-
First Name	First name of user.	-
Middle Name	Middle name of user.	-
Last Name	Last Name (Surname) of user.	This is a mandatory field. Sometimes referred to as Surname.

Note

Required fields are indicated by a red asterisk (*).

Additional User details for information purposes only:

Field	Description	Remarks
Home Telephone Number	Home telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Mobile Telephone Number	Mobile telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Contact Telephone Number	Contact telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Alternative Telephone Number	Alternative telephone number for user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Email Address	User email address.	<p>This is a mandatory field when either the conference or voicemail service is used.</p> <p>Note</p> <p>When the end user is associated with a Webex conferencing service, this email address must be unique to the end user, i.e. not previously used by any other end user/username associated with a Webex conferencing service.</p>
Job Title	Job title of user.	-
Directory Filter	-	-
Information	Additional Information for user.	-
Misc	-	-
Welcome Message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-

Step 3 After completing the relevant fields on this page, click the **Next** button.

Note

Required fields are indicated by a red asterisk (*).

Step 4 Complete the required fields and click the **Add** button. The user account is added to the database.

Available fields include:

Field	Description	Remarks
Phone Pin	The PIN to allow a user to login in to a phone with a user mobility account.	This is a mandatory field. The Pin code must be a minimum of 'n' digits (numeric characters only) - where 'n' is determined by the selected Security Profile (see above field).
Digest Credentials	Enter a string of alphanumeric characters.	Unified CM uses the digest credentials specified here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you associate the phone to the end user.
Confirm Digest Credentials	Re-enter the above credentials to confirm that you entered the digest credentials correctly.	-
Department	The end user's department.	-
Department Code	The end user's department code.	-
Ex Directory	Excludes the user from being presented in the Corporate Directory list.	Enable the checkbox to turn feature on. Disable the checkbox (default) - the feature is off.
Device Group	Determines the set of resources available to the end user at the Location.	Select from the drop-down list.
Override Language	Select a language to override the customer's default language.	Select from the drop-down list. The languages available to end users depend on the languages which were enabled at the associated customer level. When a language is selected for an end user, this language overrides the location's default language. When no language is selected for an end user, the location's default language is applied.
Feature Group	The system's Feature Group for the user.	This is a mandatory field. Select from the drop-down list. Feature Group specifies the phone and user services/functions which can be enabled for use. The list of available feature groups is defined at Customer level by the administrator who created the customer.

Field	Description	Remarks
Access Profile	Defines system menu options available for the user.	<p>Select from a drop-down list.</p> <p>Default access profile is provided as part of the product.</p> <p>The available access profiles are defined by the Provider Administrator.</p> <p>Note</p> <p>The values in the drop-down list are the values that were entered in the Description field when the Access Profiles were added to the system.</p>
Directory Partition	Select the required directory partition from the drop-down list.	-
Feature display policy	Select the required feature display policy from the drop-down list.	-
Account number to use in external accounting system	If you are using an external accounting system, enter the account number here.	-
Service Profile	Select from the drop-down list the <i>Service Profile</i> to associate to the end user.	<p>Note</p> <p>A service profile must be selected for Presence to function.</p> <p>The options available in the Service Profile drop-down list are those imported from Unified CM using the Import/Refresh Items feature, and/or from the Service Profiles added to the actual users location's IPPBX in the system.</p>
Allow control of device from CTI (Computer-Telephone integration)	To allow an end user access to phone features from CTI.	<p>Note</p> <p>This checkbox must be selected to enable Presence to control desk phones using CTI.</p> <p>Enable the checkbox to turn feature on.</p> <p>Disable the checkbox (default) - the feature is off.</p>

Manage an End User

Once a user exists in the system, the administrator can manage and add further features for each user.

The following functions can be managed for an end user (if configured):

- Single Number Reach (see [Mobile Connect/Single Number Reach \(SNR\)](#) on page 417)

- Mobile Identity (see [Mobile Identity Management on page 425](#))
- Change (Reset) Password (see [Reset User's Password on page 850](#))
- Change (Reset) user's phone PIN (see [Reset User's Phone PIN on page 851](#))
- Extension Mobility Profile (see [Extension Mobility Profiles on page 854](#))
- Presence (see *To Configure a User for Unified Presence* in [Managing a Cisco Unified Communications Manager IM and Presence \(IM and Presence\) Server on page 603](#))
- Voicemail (see [Manage Voicemail Accounts on page 867](#))
- Conference (see [WebEx Conferencing on page 873](#))
- Associate Device (see [Associate/Unassociate \(or Delete\) Device with/from User on page 852](#))
- UC Central (see [UC Central on page 874](#))

Procedure

Manage an End User

- Step 1** Find the user you want to manage and select the user by selecting the relevant *Username* active text link. The following fields are available when modifying a user:

Field	Description	Remarks
User Account locked (select to unlock)	Available only when the user account is locked.	Available only when the user account is locked. Select the checkbox to unlock the user's account.
Username	The user who you are dealing with / modifying.	This is a read-only field. Note If a user group is associated with the user (only available from system version 8.0), the specified user group is automatically displayed adjacent to the username field to create a unique username, for example; username@usergroup.
Role	The type of user as defined when the user was created.	This is a read-only field.
Security Profile	The security profile related to the user.	Select from the drop-down list if required. Options include security profiles that have been configured for your system as well as the None and Default options.
Title	Title of user.	-
First Name	First Name of user.	This is a mandatory field when either the conference or voicemail service is used.
Middle Name	Middle name of user.	-
Last Name	Last name (Surname) of user.	This is a mandatory field. Sometimes referred to as Surname.

Field	Description	Remarks
Home Telephone Number	Home telephone number of user.	-
Mobile Telephone Number	Mobile phone number of user.	-
Contact Telephone Number	Contact telephone number of user.	-
Alternative Telephone Number	Alternate contact number for user.	-
Email Address	User email address.	<p>This is a mandatory field when either the conference or voicemail service is used.</p> <p>Note</p> <p>When the end user is associated with a Webex conferencing service, this email address must be unique to the end user, i.e. not previously used by any other end user/username associated with a Webex conferencing service.</p>
Job Title	Job title of user.	-
Directory filter	Filter to be applied to the directory.	-
Information	-	-
Misc	-	-
Welcome message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-
Department	of user	-
Department Code	of user	-
Ex directory	Excludes the user from being presented in the Corporate Directory list.	<p>Enable the checkbox to turn feature on.</p> <p>Disable the checkbox (default) - the feature is off.</p>

Field	Description	Remarks
Override Language	The language to override the customer's default language.	<p>Select from the drop-down list.</p> <p>The languages available to end users depend on the customer's licensed languages.</p> <p>The languages available to end users depend on the languages which were enabled at the associated customer level. When a language is selected for an end user, this language overrides the location's default language. When no language is selected for an end user, the location's default language is applied.</p>
Feature Group	Feature Group to use for the user.	<p>This is a mandatory field. Select from the drop-down list.</p> <p>Feature Group specifies the phone and user services/functions which can be enabled for use.</p> <p>The list of available feature groups is defined at Customer level by the administrator which created the customer.</p>
Access Profile	Defines system menu options available for the user.	<p>Select from the drop-down list. Default access profile is provided as part of the product.</p> <p>The available access profiles are defined by the Provider Administrator.</p>
Directory Partition	Select the required directory partition from the drop-down list.	-
Feature display policy	Select the required feature display policy from the drop-down list.	-
Account number to use in external accounting system	If you are using an external accounting system, enter the account number here.	-
Digest Credentials	Enter a string of alphanumeric characters.	<p>Unified CM uses the digest credentials specified here to validate the credentials that the phone offers during digest authentication.</p> <p>The digest credentials that you enter in this field get associated with the phone when you associate the phone to the end user.</p>
Confirm Digest Credentials	Re-enter the above credentials to confirm that you entered the digest credentials correctly.	-

Field	Description	Remarks
Service Profile	Select from the drop-down list the <i>Service Profile</i> to associate to the end user.	<p>Note</p> <p>A service profile must be selected for Presence to function.</p> <p>The options available in the Service Profile drop-down list are those imported from Unified CM using the Import/Refresh Items feature, and/or from the Service Profiles added to the actual users location's IPPBX in the system.</p>
Allow control of device from CTI (Computer-Telephone integration)	To allow an end user access to phone features from CTI.	<p>Note</p> <p>This checkbox must be selected to enable Presence to control desk phones using CTI.</p> <p>Enable the checkbox to turn feature on.</p> <p>Disable the checkbox (default) - the feature is off.</p>
Primary Extension	Setting the primary extension is required (in Unified CM versions 8 or 9), to control a desk phone using CTI.	<p>From the drop-down list, select the extension to use as the primary extension. Default = None.</p> <p>The drop-down list displays all extensions for all devices associated to the user (phones, extension mobility profiles, analogue lines).</p>

Step 2 Make the necessary modification to the User's details, or settings within the relevant boxes. For example, the User may have changed their job title or may require a new Feature Group.

Step 3 Click the **Modify** button at the bottom-left corner of the screen.

View and Delete User Conference Account

The page enables you to view or delete a user's conference account.

Procedure

- Step 1** Browse to Location Administration > End Users.
- Step 2** Select the *Conference* link Y (active text link) of the relevant user.
- Step 3** On the next screen the conference details appear.
- Step 4** To delete the conference account, select the **Delete** button (optional).

Reset User's Password

Procedure

This process is typically used for a User that has forgotten their Password:

- Step 1** Once you have found and selected the required user, you need to access the Password screen by clicking the **Change Password** button.
- Step 2** Enter a new Password and verify it by re-entering it and clicking the **Submit** button.
-

Note

You do not need to know the old Password, as this is a reset function. You only require a new or default Password.

Once the user logs into the system with the new password, the system asks the user to change their password.

Unlocking a locked User account

When a user attempts to log into the system, the system locks the user's account after a predetermined number of unsuccessful password attempts. The number of predetermined attempts are configured via the security profile to which the user is linked.

When a user's account is locked, it is possible for an administrator to unlock the user's account. When a user's account has been locked, a message appears on the user management screen accompanied by a checkbox to unlock the account.

Procedure

To unlock a user account:

- Step 1** Browse to *General Administration > Administration Users*, or browse to *Location Administration > End Users*.
- Step 2** Select the relevant *user* (active text link).
- Step 3** On the *User Management* screen, the following message appears: *User Account Locked* (select to unlock). Select the checkbox to unlock the user's account.
- Step 4** Click the **Modify** button to complete the unlocking of the user account.

The selected user account is unlocked.

Reset User's Phone PIN

This process is typically required if a User forgets their PIN.

Procedure

- Step 1** Once you have found and selected the required user, you need to access the PIN screen by clicking the Change PIN button.
- Step 2** Enter a new *PIN*, verify it by re-entering the PIN then click the **Submit** button.
-

Note

You do not need to know the old PIN, as this is a reset function. You only require a new or default PIN.

Once the user logs into a phone with the new PIN, the system asks the user to change it.

Associate/Unassociate (or Delete) Device with/from User

Associating a device (phone or analog line) with an end user account configures the device and links it to the end user. It allows the users to customize the device settings and personalize the device. After association, the device operates as the device for the associated user until it is unassociated-associated.

The Corporate Directory shows the user with the number of the associated device.

Only one user can be associated with a specific device. However, a user can be associated with a device or multiple devices.

When associating a device to a user, please note the following:

- Devices can only be associated with an end user account.
- The device to be associated must be registered in the location.

Procedure

Associating/Unassociating (or Deleting) a Device with/from a User Account

Note

Certain phone types, for example IMS-integrated Mobile (Basic), Cisco Unified Mobile Communicator, CTI Remote Device, and Carrier-integrated Mobile are tagged with a mandatory *Owner User ID* flag, and must **always** be associated with a user. For this reason, these phone types can not be unassociated in the normal way, and the **Un-Associate** button on the relevant *Associate Device* screen is replaced with a **Delete** button. In addition to the dependencies listed below, the following actions are taken during the delete process of this type of phone.

- Phone is unregistered
- Phone is moved from the location
- Phone is deleted from phone inventory

To associate/unassociate (or delete) a device with/from a user account:

Note

If a voicemail account is tied to a specific extension number on a device associated with the user, and it is the **last instance of that extension number**, the device can only be unassociated/deleted if the voicemail account for the user is no longer active. For shared lines, where the same extension appears on multiple devices, lines/devices can be removed without affecting the voicemail service **until** there is a single instance of the extension left.

Step 1 Browse to *Location Administration > End Users*.

- Step 2** Select the required *Username* (active text link) of the user to which you want to associate/unassociate (delete) a device. The *End User Management* screen is displayed
- Step 3** Click the **Associate Device** button. The *Associate Device* screen is displayed showing a list of devices that are currently not associated with another user account. The following details are available per device in this list:

Field	Description	Remarks
Device Type	The type of device.	-
Device Name	Name of the device	-
Extension	Internal Extension	If a device is registered with more than one line, each extension number is displayed within the list.
Description	Device location information	Information / comment field (optional) which can be updated at the time of registering the phone.
Port Number	The port number of the device to which the extension is allocated.	-
Status	Associated / Not Associated	If Associated is shown - this device is already associated with this user. You can see only the devices which are associated with the specific user you manage currently. Devices already associated with other users do not appear in this list.

- Step 4** Identify the device(s) you want to associate/unassociate (delete).

Note

In case the number of unassociated devices in the location is large, you can refine the search based on all/part of the Device Name or all/part of the *Description* field (comment/information field).

- Step 5** **Note**

From version 8.1.1, CUCDM provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the user account being associated with the device:

- Logout End User. An end user logged into a device using BVSM Roaming is logged out.

Note

If the end user is logged into the Unified CM extension mobility feature, i.e. BVSM Roaming is not selected, then there is no cascade delete warning, and the end user is **not** logged out of the device. In this instance, the **end user must first log out of the device from the Unified CM** before executing the transaction.

- UC Central. Deactivate and delete UC Central feature if the line is not cloned.
- Voicemail Account. The voicemail account is removed if the end user associated with the extension mobility profile phone is the owner of the voicemail account, and the line being deleted is the primary voicemail account number.
- Single Number Reach. Delete line from destination profiles, if the line is not cloned and not already shared by another device or mobility profile of the same end user. If it is the last line of the remote destination profile the entire remote destination profile is deleted.

Note

The confirmation popup screen only indicates when a given line is deleted from a remote destination.

- Mobile Identity. Cascade delete the mobile identity associated with the line being deleted.
- Presence Monitoring. When the line being deleted is monitored for presence, deleting the line automatically removes presence monitoring on the line without any confirmation. The presence service is linked with the end user and not individual lines, and remains enabled.

Click the **Associate** button on the appropriate row to associate a device with the user OR click the **Un-Associate** or **Delete** button (as applicable) on the appropriate row to unassociate/delete a device from a user.

Step 6 If you click the **Un-Associate** or **Delete** button, a confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies, the device is immediately unassociated or deleted (as applicable).

Step 7 Click the **Un-Associate** or **Delete** button on the confirmation popup screen to continue with the unassociate/delete a device process, CUCDM removes/clears the relevant associations and unassociates/deletes the device. Alternatively click the **Cancel** button to abort the process.

Note

The unassociate/delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

Note

When a device has multiple lines, it appears multiple times in the list. However, association / unassociation of any of the lines from such a device affect all the lines. You need to act only on one line.

See also:

- [GUI Phone Registration on page 781](#).

Extension Mobility Profiles

Extension mobility profiles, often referred to as roaming profiles, enable a user to log onto a phone in another location and the phone automatically adopts the profile for that user. An extension mobility profile is required for users who move between locations on a regular basis, or for users in an organization or location, who have been assigned an extension mobility profile rather than a permanent phone.

Extension mobility profiles allow for the personalization of the following for each user:

- Profile details
- Phone lines
- Speed Dials
- Busy Lamp Fields

- Service URLs
- Line services and features
- Display name ASCII, Label ASCII and Alerting Name ASCII

The Extension mobility profile overall status is available from the user list. The value in the *Extension Mobility* column shows the status of the extension mobility profile of the user:

- **Add:** The user does not have an extension mobility profile yet.
- **Value:** The user has an extension mobility profile with an extension number as shown
- **In Service (default):** The extension mobility profile is active and can be used.
- **Out of Service:** The extension mobility profile is out of service and cannot be used.

See also:

- [Find a User on page 839.](#)

Note

Extension mobility profiles are activated in the system using two key settings, *Allow User Login* and *User Mobility*, both in the feature group. Do not activate the *Allow User Login* settings for phones that cannot support extension mobility. The Unified CM may return errors if the feature group contains mobility settings that phones in that feature group are not able to do.

Procedure

Managing an Extension Mobility Profile

Notes for managing extension mobility profiles with cloned lines:

- Line settings can only be changed for the original line, not the clones.
- All line settings changed for a line, automatically apply for the clones of that line, if any.
- Line details are suffixed with '(Clone)' if the line in question is a clone.

To manage an existing extension mobility profile:

Step 1 In the User list, select the *user* whose mobility profile you would like to manage.

Step 2 Click the **Extension Mobility Profile** button.

Via the resulting screen you can review and update the user extension mobility profile specific details and services. This page includes the following sections and options:

- Extension Mobility Profile Details
- Line Details
- Busy Lamp Fields
- Speed Dials
- Line Features and Services
- Display name ASCII, Label ASCII and Alerting Name ASCII

Note

- The call forwarding options set in the system are automatically provisioned as call forwarding options in Cisco Unified Communications Manager (Unified CM). However, if the checkbox for any call forward to Voice Mail scenario is enabled, but a destination number

for the corresponding scenario is also provided, then both are provisioned on Unified CM, but the call forward to Voice Mail setting overrides the destination number.

The *Call forward all calls to voicemail* setting takes precedence over all other call forward settings, and the *Call forward - always* setting takes precedence over all other call forward settings, **except** *Call forward all calls to voicemail*.

- If there is no connectivity between the system and Unified CM, then an error message is displayed next to the *Call forward all calls to voicemail* field, informing you that these values may be out of sync. In this case, an additional button **Sync with Call Manager** is provided next to the **Modify** button at the bottom of the page. Click the **Sync with Call Manager** button to manually sync these values with Unified CM when connectivity has been restored. The *Call forward - always* field is synced in a similar manner to the *Call forward all calls to voicemail* field.

Step 3 After updating the required details, click the **Modify** button to apply your changes.

The fields available in this section of the screen are related to the Extension Mobility Profile itself. Some are *read-only* and others are available for update.

Update Extension Mobility Profile Details		
Field	Description	Remarks
Username	User to which the Extension Mobility Profile belongs.	This is a read-only field.
Feature Group	The feature group to which the Extension Mobility Profile belongs.	This is a read-only field.
Extension Mobility Profile Name	A name to describe the profile.	This is a read-only field.
Description	A short description of the profile.	-
Phone Type	The Phone Type allocated to this Mobility profile.	Select from the drop-down list.
Button Template Name	Cisco Unified CM includes several default phone button templates. When adding phones, you can assign one of these templates to the phones.	Select from the drop-down list. The system automatically presents button templates based on the Phone Type selected. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones. For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial.
Softkey Template	Softkey template configuration allows the administrator to manage softkeys that the Cisco IP Phones (such as model 7960) support.	Select from the drop-down list. The default Softkey template for the phone was selected as part of a Feature Group. However, you may be able to select them per phone as well, overriding the feature group setting.

Update Extension Mobility Profile Details		
Field	Description	Remarks
Phone Locale	The locale that affects the language displayed on the phone LCD.	<p>The values are based on the Unified CM supported languages.</p> <p>The language in which the phone screens are displayed is dependent upon:</p> <p>The available languages loaded on the system.</p> <p>The availability of the system's XML screens in the required language.</p>
Privacy	When privacy is enabled (select <i>On</i>), the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls.	This feature is only available if it is selected in the relevant Feature Group.
First Expansion Module Type	Primary expansion module type to be used by phone.	<p>This is an optional field.</p> <p>This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.</p>
Second Expansion Module Type	Secondary expansion module type to be used by phone.	<p>This is an optional field.</p> <p>This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.</p>
Extension Mobility Cross Cluster	Determines whether the user is enabled for cross-cluster roaming.	<p>Select or clear this checkbox to enable or disable the user for cross-cluster roaming.</p> <p>This checkbox is only visible for a user when the <i>Value Add/Extension Mobility Cross Cluster</i> checkbox is selected (enabled) on the <i>Manage Feature Group</i> screen for the relevant feature group. Default = disabled (not selected).</p>

Phone Layout. The *Phone Layout* section lists all the available buttons, with the associated button type and line details. When the phone has one or more expansion modules a separator line separates phone buttons from expansion module buttons. From this section you are able to Manage Lines, Manage Speed Dials, Manage Busy Lamp Fields and Manage Service URLs.

Note

The Phone Layout section is based on the button display layout, and only appears in this format when: The button templates are imported from Unified CM. The Phone Layout is also based on the phone's Feature Group settings.

Line Features (per line)

- The Settings section lists all of the lines associated with the phone and enables you to modify the line settings for Private line settings, Common line settings, and Common line settings (Call Forward). These settings include Label, ASCII Label, Message waiting lamp policy, Ring setting-(active and idle), Contact Center, Display name, ASCII Display Name, Call forward settings, Forwarded Call Display settings, Music on hold, Line Class of Service, and so on. You can configure aspects such as call forwarding and line labels, display names, alerting names and the ASCII value fields for label, display and alerting name fields. The fields displayed in this section vary according to the associated feature group's settings. For example, some phone types support *Recording Profile* and *Recording Option* settings so that if the recording profile has been imported ([Importing/Refreshing CCM Items on page 87](#)), it is available on the drop-down list. The *Recording Option* list has the following options, in accordance of the version of Unified CM:
 - *Call Recording Disabled* - Unified CM 7.0 up
 - *Automatic Call Recording Enabled* - Unified CM 7.0 up
 - *Application Invoked Call Recording Enabled* - Unified CM 8.0 up
 - *Device Invoked Call Recording Enabled* - Unified CM 7.0 up

The *Forward All Secondary CoS* field in the *Common line settings..... (Call Forward)* section of the screen is only visible if the *Forward All* checkbox is selected in the *Common Line settings(Call Forward)* section of the screen in the associated feature group.

Note

Text typed in the *Label* field automatically populates the *Label ASCII* field with the same text, it also overwrites any existing text in the *Label ASCII* field. You can however edit text in the *Label ASCII* field without affecting/overwriting the text in the *Label* field.

When a Voicemail account is added to a user/line, call forward to Voicemail is enabled if no explicit call forward destination (number or URI) has been configured, that is the following Voicemail checkboxes in the *Common line settings for line n (Call Forward)* section of the screen are automatically enabled (set to true) on the selected line: *Forward Busy* (Int/Ext if applicable), *Forward No Answer* (Int/Ext if applicable), and *Forward Unregistered* (Int/Ext if applicable) if the corresponding destination field is left blank, that is no number or URI is configured [in the *Common line settings for line n (Call Forward)* section of the screen]. When a Voicemail account is added to a user/line, and the corresponding **destination has been configured** then the call forward settings on the line are left unchanged.

For shared lines, each feature listed in the Private Line settings section (now labeled *Private line settings and Shared device settings*) are associated with a checkbox that can be selected to apply private line settings to all devices on the shared line. After the selection of the required checkboxes, click the **Apply** button.

Note

Shared line support for additional services in CUCDM, for example SNR, Presence, extension mobility, and so on, is dependent on Unified CM support.

Make sure that the Unified CM you are using supports the features for the lines before attempting to provision them.

- **Example of copying a private line setting:** If the admin user enters a new value ("Line1") into the *Label* field (but does not modify this device first) and selects the *Label* and *Line Mask* checkboxes to change their values, the *Label* value changes to "Line1" and the *Line Mask* value changes to the existing blank value for all devices on the shared line. Please note that the devices need not be associated to the user. Their private line settings are changed if they share the same extension. Also note that the **Apply** button is disabled (i.e. grayed out or not selectable) until one of the checkboxes is selected. If no checkbox is selected it remains disabled. The **Apply** button only changes the private line settings for the current displayed line. It does not affect any of the other lines of the device. It is therefore not possible to select multiple settings on multiple shared lines and expect them all to be applied to all the shared lines.
- **Multiple Call/Call Waiting Settings for line.** The following fields are displayed:
 - Call waiting busy trigger
 - Cloned Lines
 - Max calls waiting

Procedure

Manage Lines

Lines are managed as follows:

Step 1 Click the **Manage Lines** button.

Step 2 Complete the form.

Field	Description
<i>Button #</i>	The configured button # for the selected device is displayed.
<i>Line</i>	Lists extensions and numbers configured for the corresponding line or order position. This field has a checkbox to provide the user the ability to move and delete multiple lines together. This field is also selectable; once selected all lines associated are highlighted in bold allowing the user to easily identify associated extensions.
<i>Action</i>	Two action buttons are displayed depending on the current line position configuration. The Add button is displayed adjacent to the <i>Button #</i> if no number has been configured for the position. The Delete button is displayed adjacent to the <i>Button #</i> if a number is configured for the button. This allows for the number to be easily removed. See under <i>Add Line</i> and <i>Delete Line</i> below for more information on the use of these buttons.

Note on use of buttons

- **Move Up and Move Down:** These buttons are used to shift positional order for the device, based on the checkbox selected next to the *Line* field, these shift either up or down depending on the button clicked. These selected items are shifted one level at a time.
- **Delete Selection:** This button is based on the checkboxes selected next to the *Line* field. Clicking it deletes the selected items.
- **Undo Changes:** This undoes all changes made during the configuration for lines and positions on the device.
- **Select None:** This button deselects all checkboxes currently selected next to the *Line* field.

- **Swap Selected:** Click this button to swap the positional order of the items whose checkboxes are selected next to the *Line* field.
- **Modify:** Click this button to implement all changes made.
- **Cancel:** This cancels out all changes made and returns the user to the *Phone Management* screen.

Step 3 Click the **Modify** button to finalize the transaction.

Add Line

Adding a line is one of the line management features.

Procedure

To add (configure) a line:

Step 1 Click the **Manage Lines** button under the *Phone Layout* section.

Step 2 Click the **Add** button to configure a number for the selected *Button #*.

Step 3 Select either the *Add Line* radio button or the *Add Clone* radio button.

Complete the following fields for the *Add Line* option:

Field	Description
Number	Select from a drop-down list the phone number associated with the line.
Label	Enter a unique label for the line.
COS	Select from the drop-down list the class of service to allocate to the line. Note When selecting a COS, the corresponding CSS must exist on Unified CM.

Complete the following fields for the *Add Clone* option:

Field	Description
Selected Line	This drop-down list is used to specify if the line is to be cloned.
Number Clones	Select the relevant number of clones that you would like to make of the line.

Step 4 Click the **Add** button when complete or the **Cancel** button to abort.

Step 5 Click the **Modify** button to finalize the transaction.

Delete Line

Procedure

To delete an extension mobility line:

Note

If a voicemail account is tied to a specific extension number on a device associated with the user, and it is the **last instance of that extension number**, the extension mobility line can only

be deleted if the voicemail account for the user is no longer active. For shared lines, where the same extension appears on multiple devices, lines/devices can be removed without affecting the voicemail service **until** there is a single instance of the extension left.

Note

From version 8.1.1, Cisco Unified Communications Domain Manager (CUCDM) provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the lines(s) being deleted from the extension mobility profile:

- Logout End User. An end user logged into a device using BVSM Roaming is logged out.

Note

If the end user is logged into the Unified CM extension mobility feature, i.e. BVSM Roaming is not selected, then there is no cascade delete warning, and the end user is **not** logged out of the device. In this instance, the **end user must first log out of the device from the Unified CM** before executing the transaction.

- UC Central. Deactivate and delete UC Central feature if the line is not cloned.
- Voicemail Account. The voicemail account is removed if the end user associated with the extension mobility profile phone is the owner of the voicemail account, and the line being deleted is the primary voicemail account number.
- Single Number Reach. Delete line from destination profiles, if the line is not cloned and not already shared by another device or mobility profile of the same end user. If it is the last line of the remote destination profile the entire remote destination profile is deleted.

Note

The confirmation popup screen only indicates when a given line is deleted from a remote destination.

- Mobile Identity. Cascade delete the mobile identity associated with the line being deleted.
- Phone Busy Lamp Field references. When deleting a line that is being monitored using a busy lamp field (on the same device or another device), those device busy lamp fields are removed (if the line is neither shared nor cloned).
- Mobility Profile Busy Lamp Field references. When deleting a line that is being monitored using a busy lamp field on one or more extension mobility profiles, the extension mobility profile busy lamp field is removed (if the line is neither shared nor cloned).
- Number (Line) Group Lines - The line being deleted is deleted from any associated number (line) groups if the line is neither shared nor cloned Pickup Group(s) - The line being deleted is deleted from any associated pickup groups (if the line is neither shared nor cloned).
- Pickup Group(s). The line being deleted is deleted from any associated pickup groups (if the line is neither shared nor cloned).
- Presence Monitoring. When the line being deleted is monitored for presence, deleting the line automatically removes presence monitoring on the line without any confirmation. The presence service is linked with the end user and not individual lines, and remains enabled.

Step 1 Click the **Manage Lines** button under the *Phone Layout* section on the *Manage Extension Mobility Profile* screen. The *Line Management* screen is displayed.

Step 2 Click the **Delete** button adjacent to the line to delete in order to delete the selected line configuration, OR select multiple lines to delete (if required) by selecting the required *Button*

checkboxes and then clicking the **Delete Selection** button. A confirmation popup screen is displayed (if applicable).

Note

If there are no associated dependencies and you wish to delete the line/s, proceed with step 6, that is simply click the **Modify** button.

- Step 3** Click the **Delete Selection** button on the confirmation popup screen to continue with the delete line/s process. Alternatively click the **Cancel** button to abort the process.

Note

The delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

- Step 4** Reconfigure the line if required (see *Add Line* above).
- Step 5** Repeat the above steps to delete and/or reconfigure another extension mobility line (if required).
- Step 6** Click the **Modify** button on the *Line Management* screen when complete to reapply the line configuration, or to delete the extension mobility line/s (including all dependencies) without reconfiguring - as appropriate.

Procedure

Modifying an Extension Mobility (Roaming) Profile's Alerting Name/Alerting Name ASCII

Note

Before attempting to manage an alerting name, please ensure that Alerting Names are enabled in the active Feature Group.

To modify an Alerting Name:

- Step 1** Browse to the relevant user's extension mobility profile via *Location Administration > End Users*.
- Step 2** In the *Alerting Name* and *Alerting Name ASCII* fields, enter the required Alerting Name and ASCII value for Alerting Name ASCII.
- Step 3** Click the **Modify** button. The extension mobility profiles alerting name is updated.

Procedure

Deleting an Extension Mobility Profile

Note

From version 8.1.0, Cisco Unified Communications Domain Manager (CUCDM) automatically removes/clears the following elements associated with an extension mobility profile during the delete extension mobility profile process:

- Speed dials
- Busy lamp fields
- Service URL's

- IP phone service subscriptions

In addition to this, from version 8.1.1, CUCDM provides a cascade delete confirmation summary popup screen that details the actions taken to automatically modify or remove related services that depend on the extension mobility profile being deleted:

- Delete mobility lines (for details see dependencies under [Procedure 37, “” on page 860](#))

- Step 1** Select the required *Username* (active text link) for whom you wish to delete the extension mobility profile.
- Step 2** Click the **Extension Mobility Profile** button. The *Manage Extension Mobility Profile* screen is displayed.
- Step 3** Click the **Delete** button (located at the bottom-right of the screen). A confirmation popup screen is displayed listing the configured dependencies (if applicable).

Note

If there are no associated dependencies, the extension mobility profile is deleted immediately.

- Step 4** Review the associated dependencies and click the **Delete** button on the confirmation popup screen to continue with the delete process. The extension mobility profile (including all associated dependencies) is deleted. Alternatively, click the **Cancel** button to abort the process.

Note

The delete transaction is disallowed, and an appropriate message is displayed on the confirmation popup screen if the user does not have the necessary permission to delete one or more of the dependencies.

See also:

- [Find a User on page 839](#).
- [Manage an End User on page 846](#).
- [Manage IP Phone Service Subscriptions on page 385](#).

Adding an Extension Mobility Profile

Please note the following before adding an extension mobility profile to a user account:

- An Extension Mobility Profile name cannot be the same as a device name on Unified CM, since both are device types. Device types require distinct names. Adding a profile name that is the same as an existing device name will result in an error and the profile will not be added.
- The feature group associated with the user account must have *User mobility* enabled by the customer administrator.
- The location associated with the user account must have sufficient *Mobility Profile Service* inventory available. Service inventory levels for *User Mobility* resources are assigned by an administrator or a higher level in the hierarchy.
- When adding extension mobility as a shared line the COS value is inherited from the shared line and becomes read-only. Shared line support for additional services in CUCDM, for example SNR, Presence, extension mobility, and so on, is dependent on Unified CM support. Make sure that the Unified CM you are using supports the features for the lines before attempting to provision them.

Procedure

To add an extension mobility profile to a user account:

- Step 1** On the relevant *User Management* screen, click the **Extension Mobility Profile** button. Alternatively, click the *Add* link (active text link) in the *Extension Mobility* column of the user list.
- Step 2** Fill in the information on the following screen and click the **Next** button. The following fields are available:

Field	Description	Remarks
Username	User to which this extension mobility profile belongs.	This is a read-only field.
Description	A short description of the profile.	
Feature Group	Feature Group with which the user was created.	This is a read-only field. The feature group affects the information displayed in the next sections of the screen.
Limits outbound calls to	The Class of Service definition for outgoing calls as defined in the feature group for the user.	-
Phone Type	The Phone Type allocated to this Mobility profile.	Select from the drop-down list.
Button Template Name	Cisco Unified CM includes several default phone button templates. When adding phones, you can assign one of these templates to the phones.	Select from the drop-down list. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones. For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial.
Softkey Template	Softkey template configuration allows the administrator to manage softkeys that the Cisco IP Phones (such as model 7960) support.	Select from the drop-down list. The default Softkey template for the phone was selected as part of a Feature Group. However, you may be able to select them per phone as well, overriding the FG setting.
Privacy	When privacy is enabled (select <i>On</i>), the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls.	This feature is only available if it is selected in the relevant Feature Group.

Field	Description	Remarks
Expansion Module 1	Primary expansion module type to be used by phone.	This is an optional field. This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.
Expansion Module 2	Secondary expansion module type to be used by phone.	This is an optional field. This drop-down list only appears when the Phone Type selected has protocol 'SCCP' and 'Expansion Module Capable' selected.
Extension Mobility Cross Cluster	Determines whether the user is enabled for cross-cluster roaming.	Select or clear this checkbox to enable or disable the user for cross-cluster roaming. This checkbox is only visible for a user when the <i>Value Add/Extension Mobility Cross Cluster</i> checkbox is selected (enabled) on the <i>Manage Feature Group</i> screen for the relevant feature group. Default = disabled (not selected).
Line	The line	As a user can have multiple lines, the details in this row apply to "lineX" of the user.
Label	The line label if configured (leave blank for default).	Label
Label ASCII	An ASCII value for the line's label.	

Field	Description	Remarks
Line Class of Service	Line Class of Service	<p>Select the relevant line class of Service from the drop-down list. By default, the <i>Default</i> class of service, as specified in the feature group, is used.</p> <p>Note</p> <ul style="list-style-type: none"> Any changes to the feature group values or settings, whether modified in the Feature Group Management section or via OpsTools, are not applied to the COS of a registered line. When adding extension mobility as a shared line the COS value is inherited from the shared line and becomes read-only. Although shared analog lines can be allocated across all protocols, SIP and H323 may give unexpected results due to limited support in the Unified CM.

Note

The exact layout on the screen depends on whether the *Button Display Mask* option is selected in the end user's feature group or not. The *Button Display Layout* presents line's details in relation to the associated phone button.

- Step 3** Select the *Number* for each available line and click the **Next** button.
- Step 4** Enter the Label for each line number and select the Line Class of Service, and then click the **Add** button.

See also:

- [Managing Numbers on page 884.](#)

Speed Dials

This page enables you to manage the speed dial numbers associated with the mobility profile.

Procedure

Add a New Speed Dial Number

Follow these steps:

- Step 1** Complete the required fields
- Step 2** Select the **Add** button

The speed dial number will be added to the mobility profile.

Procedure

Clear all Configured Speed Dials

Follow these steps:

- Select the **Clear** button

All speed dials will be cleared from the mobility profile.

Add Busy Lamp Field

Procedure

To add a new Busy Lamp Field:

- Step 1** Complete the required fields.
- Step 2** Select the **Add** button

The Busy Lamp Field will be added to the mobility profile.

The following fields are available:

Field	Description
Busy Lamp Field number	The number that this busy lamp field is associated with.
Label	A label for the busy lamp field.
Label (ASCII)	An ASCII value for the BLF. Note: If the ASCII Label field is not provided and the standard Label field has a valid ASCII value then the standard Label field's value is used for the ASCII Label field; but if the standard label is not a valid ASCII value then the Telephone Number field's value is used for the ASCII Label field. If the Label field is not provided and the ASCII Label field has a valid ASCII value then the ASCII Label field's value is used for the standard Label field; but if the ASCII Label field is not a valid ASCII value then the Telephone Number field's value is used for the Label field.
Telephone Number	The telephone number associated with the speed dial short cut key.
Call Pickup	Select the checkbox to enable call pickup for the BLF.

Manage Voicemail Accounts

IP Voicemail (VM) enables callers to leave messages for the user when a phone is unanswered or diverted to the Voicemail system and the User can then retrieve the message when he/she is available. Additionally, voicemail allows the user to personalize their responses in case they cannot answer the phone providing callers with information regarding his or her whereabouts or expected availability.

Only users with a phone number can have a VM account. Therefore, before creating a VM account for a user, the user must have a Mobility profile or be associated with a phone.

Note

- It is important to refer to the LDAP Integration Guide, specifically in relation to the limitations and prerequisites of user voicemail account management (adding, modifying and deleting) when Cisco Unity Connection is LDAP integrated.
 - Only personal VM is currently available.
-

See also:

- [Adding an Extension Mobility Profile on page 863.](#)
- [Associate/Unassociate \(or Delete\) Device with/from User on page 852.](#)

See [Create Voicemail Account on page 870](#) for field details.

You can reset the voicemail PIN in case the user forgets their PIN. Once done, the voicemail box requires the user to change their PIN similar to the 1st time they used their voicemail box.

Procedure

Update PIN

To update the voicemail box PIN:

- Step 1** Select the **Y** in the *Voicemail* column of the relevant user on the *User Management* screen (see also [Find a User on page 839](#)). Alternatively, click the **Voicemail** button on the relevant user's *User Management* screen.
- Step 2** Click the **Personal Voicemail** button or the **Y** next to Personal Voicemail.

Note

The new Voicemail PIN **must be different** from the current Voicemail PIN in order for it to be updated and unlocked on the Voicemail server. Leave this field blank if you want to keep your original PIN. This is an optional field when managing your voicemail account, and must only be completed if you want to change your voicemail PIN.

- Step 3** Update the PIN and click the **Modify** button.
-

Procedure

Update Voicemail Profile

To update the voicemail profile:

- Step 1** Select the **Y** in the *Voicemail* column of the relevant user on the *User Management* screen (see also [Find a User on page 839](#)). Alternatively, click the **Voicemail** button on the relevant user's *User Management* screen.
- Step 2** Click the **Personal Voicemail** button or the **Y** next to Personal Voicemail.
- Step 3** Select the required voicemail profile from the drop-down list and click the **Modify** button.
-

Procedure

Delete User Voicemail Account**Note**

If the Username is referenced in the Caller Input of another user, the reference must first be removed before the Voicemail account can be deleted.

This includes the user personalization details, and any messages saved or new. To delete the user voicemail:

- Step 1** Select the **Y** in the *Voicemail* column of the relevant user on the *User Management* screen (see also [Find a User on page 839](#)). Alternatively, click the **Voicemail** button on the relevant user's *User Management* screen.
- Step 2** Click the **Personal Voicemail** button or the **Y** for the user's personal Voicemail
- Step 3** Click the **Delete** button.

Manage Caller Inputs**Procedure**

To manage caller inputs:

- Step 1** Click the **Caller Input** button on the *Manage Voicemail Accounts* screen.
- Step 2** The *Manage Voicemail Account* screen displays columns for the input keys as well as existing entries, showing the call action (Transfer, Ignore, or Goto) as well as the target phone number or username.

To edit or modify a key, select the relevant caller input key (active text link) to open the *Caller Input* screen.
- Step 3** On the *Caller Input* screen, enter the required caller input details as follows:
 - a** If you want to route the call to another contact number, select the *Call Action* radio button and choose the required action from the drop-down list, namely *Ignore* or *Transfer To Alternate Contact Number*. Then, in the *Extension* field, enter the contact number to which the call must be transferred (if applicable). This is a mandatory field.

Note

The extension number must be entered if the *Call Action* is set to *Transfer To Alternate Contact Number*.

- b** Alternatively, if you want to route the call to a user extension, select the *User with Mailbox* radio button, and enter the Username to whom you want to route the call. Then, select the relevant radio button to perform the action required, namely *Attempt Transfer* or *Go directly to Greetings*, which determines whether the call transfers to the user extension or goes directly to the user greeting respectively.

Note

The Username must belong to the same Customer as you, and must also reside on the same Voicemail server.

- Step 4** Click the **Submit** button when complete to update the caller input key details in the system.

Voicemail Notification**Procedure**

Manage Alternate Extensions

To manage alternate extensions:

- Step 1** Select the *Y* active text link in the *Voicemail* column of the relevant user on the *User Management* screen (see also [Find a User on page 839](#)). Alternatively, click the **Voicemail** button on the relevant user's *User Management* screen.
- Step 2** Click the **Personal Voicemail** button or the *Y* next to Personal Voicemail.
- Step 3** Click the **Alternate Extensions** button.
- Step 4** Click the **Add** button (if required) to add a new alternate extension for the user, then enter the required alternate extension number in the *Alternate Extension* field and then click the **Add** button to submit the entry to the system.
- Step 5** Click the **Delete** button adjacent to the alternate extension if you want to delete an alternate extension. The selected alternate extension is deleted from the system.

Procedure

Manage Notifications**Note**

For notifications to work correctly in CUCDM, the Cisco Unity Connection server **must be configured** to facilitate the required notifications.

To manage notifications:

- Step 1** Select the *Y* active text link in the *Voicemail* column of the relevant user on the *User Management* screen (see also [Find a User on page 839](#)). Alternatively, click the **Voicemail** button on the relevant user's *User Management* screen.
- Step 2** Click the **Personal Voicemail** button or the *Y* active text link next to Personal Voicemail.
- Step 3** Click the **Notifications** button.
- Step 4** Enter the following (as required):
- Display Name - enter the required display name for the notification.
 - Notification type [SMS, Phone, Email (SMTP), or Pager] - from the drop-down menu.
 - Status (Enabled or Disabled) - select the appropriate radio button.
 - Destination - the notification destination (mandatory field).
 - From - typically the name of the person sending the notification. Available for SMS and Email notification types only.
 - Send (text) - to display to user. 160 characters maximum
 - Include Message Information in Message Text - select/deselect checkbox as required. Available for SMS and Email notification types only.
 - Include Message Count in Message Text - select/deselect checkbox as required. Available for SMS and Email notification types only.
- Step 5** Click the **Add** button when complete to submit the notification entry to the system.

Create Voicemail Account

IP Voicemail enables callers to leave messages for the user when a phone is unanswered or diverted to the voicemail system and the User can then retrieve the message when he/she is

available. Additionally, voicemail allows the user to personalize their responses in case they cannot answer the phone providing callers with information regarding his or her whereabouts or expected availability.

Only users with a phone number can have a voicemail account. Therefore, before creating a voicemail account for a user, the user must have a Mobility profile or be associated with a phone.

Note

- It is important to refer to the LDAP Integration Guide, specifically in relation to the limitations and prerequisites of user voicemail account management (adding, modifying and deleting) when Cisco Unity Connection is LDAP integrated.
 - Only personal voicemail is currently available.
-

See also:

- [Adding an Extension Mobility Profile on page 863.](#)
- [Associate/Unassociate \(or Delete\) Device with/from User on page 852.](#)

Procedure

Create Voicemail Account

To create a voicemail account:

- Step 1** Click the **Add** button under the *Voicemail* column on the *User Management* screen. **Alternatively**, on the user account management screen, click the **Voicemail** button.
- Step 2** Click the **Personal Voicemail** button or the *Add* key (active text link) to access the personal user voicemail.
- Step 3** Update the required fields (see below), and click the **Add** button when complete.

Field	Description	Remarks
Username	User for which you are creating the voicemail account.	This is a read-only field.
PIN (numeric values)	PIN for the use of Voicemail when accessed from a phone.	This is a mandatory field when adding (creating) a voicemail account. This is an initial PIN and the Voicemail system asks the user to change their PIN the first time they access their voicemail box.
Self Enroll on next login	Select the required self enroll option from the drop-down list.	This field is only available when modifying a voicemail account. Options available are: Disabled - sets this setting to OFF on the Cisco Unity Connection server, Enabled - sets this setting to ON on the Cisco Unity Connection server, and Ignore - does not change the setting on the Cisco Unity Connection server.

Field	Description	Remarks
Voicemail Profile	Select the required voicemail profile from the drop-down list.	This is a mandatory field when adding (creating) a voicemail account.
Line Number	The phone line to which this voicemail box is linked.	<p>This is a mandatory field when adding (creating) a voicemail account. As a user can have multiple lines, you can set up their voicemail box for any of their lines.</p> <p>The number the user dials to retrieve voicemail messages, is based on this line's number, but prepended by the site code (SLC). Thus, voicemail box number = SLC+extension.</p> <p>Note</p> <ul style="list-style-type: none"> • A user can only have one voicemail box regardless of the number of lines it has. • Call forward to Voicemail is enabled if no explicit call forward destination has been configured in the <i>Common line settings for line n (Call Forward)</i> section of the screen, i.e. the following Voicemail checkboxes in the <i>Common line settings for line n (Call Forward)</i> section of the screen are automatically enabled (set to true) on the selected line: <i>Forward Busy</i> (Int/Ext if applicable), <i>Forward No Answer</i> (Int/Ext if applicable), and <i>Forward Unregistered</i> (Int/Ext if applicable), if the destination field is left blank. If the corresponding destination field has been configured then the call forward settings on the line are left unchanged.

Field	Description	Remarks
Voicemail Template	The Voicemail template, to associate with this voicemail box.	<p>This is a mandatory field when adding (creating) a voicemail account. Select from the drop-down list</p> <p>Default based on voicemail profile defined in the user feature group.</p> <p>The voicemail template defines the setting of the voicemail box. For example: voicemail box size (MB), max number of messages, for how long to keep message history etc.</p>

Single Inbox

Single Inbox is a Cisco Unity Connection 8.5 feature that enables users to have a single inbox in their e-mail client that is used for their e-mail as well as their voicemail.

Note

- Users must have valid email addresses configured for this feature to work correctly. If this feature is activated for a user that does not have an email address provisioned, the system provisions the Single Inbox functionality for the user but it is not activated.
- The Single Inbox functionality is only visible to users whose voicemail is provided by a Cisco Unity Connection 8.5 server. The *Unified Messages Service* drop-down list under the *Single Inbox* section on the *Create Voicemail Account* or *Manage Voicemail Account* screens is not visible to users who do not have access to the Single Inbox functionality.

Procedure

To activate Single Inbox:

- Step 1** Select the required service from the *Unified Messaging Service* drop-down list.

Note

If the Single Inbox Feature is not available, make sure that you are using Cisco Unity Connection 8.5 and that the Single Inbox feature has been enabled.

- Step 2** Click the **Add** button. Single Inbox is activated for the selected user.

See also: [Manage Voicemail Accounts on page 867](#)

WebEx Conferencing

The system provides functionality to allow end users access to Cisco WebEx conferencing, via the system interface.

Procedure

To add the WebEx service to an End User:

- Step 1** Browse to *Location Administration > End Users*.

- Step 2** Select the *Username* (active text link) of the relevant user.
- Step 3** Click the **Conference** button on the User Management screen.
- Step 4** Select the relevant WebEx service option from the Conference Service drop-down list then click the **Next** button.

Note

The type of conference service available depends on the conference services that have been added to the system and made available to the end user's location. It could include IPUnity and WebEx conference services.

- Step 5** A confirmation of the WebEx service being added for the user is displayed, click the **Add** button.
- WebEx is now added to the user's profile in the system and the user's details are registered on the WebEx remote service.

The following WebEx fields are set using information available to the system or via static configuration:

Webex Parameter	System Parameter	Fixed
firstName	user/firstName	
lastName	user/lastName	
title	user/title	
description	Information	
company	customer/customerName	
webExId	userName	
email	emailAddress	
password	password	
active		ACTIVATED
		Note When the end user is registered on WebEx, the account status is activated.

With the exception of the user's password, these fields are not updated in WebEx when it is modified in the system. The modifications need to be done separately in WebEx.

UC Central

Before an administrator can enable an extension for UC Central, the end user must either have a registered device or a Mobility profile.

Procedure

Enabling a User's extension as a UC Central extension

To enable a user's extension as a UC Central Client extension:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the required *User*.
- Step 3** Click the **UC Central** button.

Note

The default is *No Extension Selected* if the user has not yet selected an extension to be enabled as a UC Central Client extension.

Step 4 Select one of the extensions to be enabled as a UC Central Client extension.

Note

A cloned line **can be enabled** as a UC Central extension, however a shared line **can not** be enabled as a UC Central extension.

Step 5 Click the **Add** button.

Note

For Self Care, if the user has UC Central enabled in the feature group, the *UC Central* link is available in the Self Care menu, and the user can enable an extension for UC Central there.

Note

- Once the **Add** button is clicked, the extension is only marked as enabled for UC Central. The actual activation processing only happens when the UC Central administrator sends an activation request to process the UC Central enabled extensions. This is done via API's and not the GUI interface.
- Existing SNR configuration on the enabled line is removed and the new SNR configuration is added.
- Once activated, the user is not able to make any changes to the UC Central extension.

On clicking the **Add** button, the following back-end transactions are triggered:

- *AddInterwiseClient* (for more information see the UC Central Provisioning Guide)
- *InterwiseClientActivation* (for more information see the UC Central Provisioning Guide)

Procedure***Modifying the extension used for UC Central***

To modify the extension used for UC Central (i.e. to enable a different extension as the UC Central Client extension), follow the steps below:

Step 1 Browse to *Location Administration > End Users* .

Step 2 Select the required *User*.

Step 3 Click the **UC Central** button.

Step 4 Select one of the extensions to be enabled as a UC Central Client extension.

Step 5 Click the **Apply Changes** button.

Note

- Once the **Apply Changes** button has been clicked, the extension is only marked as enabled for UC Central. The actual activation processing only

happens when the UC Central administrator sends an activation request to process the UC Central enabled extensions. This is done via API's and not the GUI interface.

- Existing SNR configuration on the enabled line is removed and the new SNR configuration is added.
- Once activated, the user is not able to make any changes to the UC Central extension.

On clicking the **Apply Changes** button, the following back-end transaction is triggered:

- *InterwiseClientLineMod* (for more information see the UC Central Provisioning Guide)

Procedure

Disabling a User's extension as a UC Central extension

To disable a user's extension as a UC Central Client extension:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the required User.
- Step 3** Click the **UC Central** button.
- Step 4** Select the Disable UC Central option.
- Step 5** Click the **Apply Changes** button.

On clicking the **Apply Changes** button, the following back-end transaction is triggered:

- *DelUserInterwiseClient* (for more information see the UC Central Provisioning Guide)

Procedure

Deactivating a User's UC Central connection

To deactivate a user's UC Central connection:

- Step 1** Browse to *Location Administration > End Users*.
- Step 2** Select the required *User*.
- Step 3** Click the **UC Central** button.
- Step 4** Click the **Deactivate** button.

On clicking the **Deactivate** button, the following back-end transaction is triggered:

- *InterwiseClientDeactivation* (for more information see the UC Central Provisioning Guide)

Note

When UC Central is deactivated for a user, the extension remains enabled for UC Central.

Administration Users

This section covers the management of Administration users.

Add an Admin User

When you create an Admin user from the *General Administration* menu, a user account with an Admin role is added to the database.

Note

An Administrator can only add a new administrator or modify an existing administrator at a level lower than his or her own level in the administration hierarchy.

The User Management page displays the existing user accounts for the current location.

Note

A red asterisk adjacent to a field indicates that it is a mandatory field

Procedure

To add a new end user:

- Step 1** Click the **Add** button at the top of the *User Management* screen. The *Add Administrator* screen is displayed.
- Step 2** Enter the user's details. The fields available in this section of the screen are to do with basic user information:

Field	Description	Remarks
Username	The id of the user.	<p>Must be unique across the platform, and is a mandatory field.</p> <p>Best Practice: Consider implementing a user name convention.</p> <p>Note</p> <p>Once a user group has been configured for a customer, the usernames of all end-users added at the relevant customer are automatically combined with the user group to create a unique user name, for example username@usergroup; where the username (entered in this field) is displayed adjacent to the user group (already configured by the System, Provider or Reseller administrator).</p> <p>See also the <i>UsernameValidation</i> setting at Provider Preference and Settings on page 937.</p>
Security profile	The security profile related to the customer.	This is an optional field. Options include security profiles that have been configured for your system as well as the None and Default options.

Field	Description	Remarks
Password	Initial password for user login into the GUI.	This is a mandatory field.
Role	User role in the platform.	<p>Select from the drop-down list.</p> <p>User can only have one role. The user role defines what "type" of user they are and what sort of functions they can perform in the system.</p> <p>For example:</p> <p>Location Administrator</p> <p>Note</p> <p>Administrators can only add a new administrator at a level lower than their own level in the administration hierarchy. Location administrators therefore do not have the option of adding a new admin user.</p>
Web service access	Identifies the user's credentials for use by Web services API's, for example a 3rd Party system registering a phone.	<p>This is an optional field.</p> <p>Checkbox selected = Enabled (Web service access allowed), Checkbox not selected = disabled (not allowed).</p>
Title	Title of user.	-
First name	First name of user.	-
Middle name	Middle name of user.	-
Last name	Last name (surname) of user.	This is a mandatory field. Sometimes referred to as "Surname".
Home telephone number	Home telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Mobile telephone number	Mobile telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Contact telephone number	Contact telephone number of user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.
Alternative telephone number	Alternative telephone number for user.	This field is limited to 32 characters and can contain alphanumeric and non-alphanumeric characters.

Field	Description	Remarks
Email address	User email address.	This is a mandatory field when either the conference or voicemail service is used. Note When the end user is associated with a Webex conferencing service, this email address must be unique to the end user, i.e. not previously used by any other end user/username associated with a Webex conferencing service.
Job title	Job title of user.	-
Directory filter	Filter to be applied to the directory	-
Information	Additional Information for user.	-
Misc	-	-
Welcome message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-

Step 3 After completing the relevant fields on this screen, click the **Next** button.

The fields available on the second page include:

Field	Description	Remarks
GUI Branding	The branding theme (colors, fonts, items look & feel etc.) to be presented to the user when they log in to the GUI.	Select from the drop-down list The branding themes are defined by the Provider administrator. The applicable branding themes should be enabled for each level in the hierarchy.
Preferred country	Displays the preferred country.	Select from the drop-down list.
Access profile	Defines menu options available for the user.	Select from the drop-down list. The available access profiles are defined by the Provider Administrator. Default access profile is provided as part of the product.
Account number to use in the external accounting system.	The account number to use in the external accounting system.	Enter the account number to use in the external accounting system.

Step 4 Complete the required fields and click the **Add** button. The user account is added to the system.

Manage an Admin User

The *User Management* screen enables you to manage user profiles.

Note

An Administrator can only add a new administrator or modify an existing administrator at a level lower than his or her own level in the administration hierarchy.

Procedure

To manage a user:

Step 1

Modify the required fields. Fields available on the User Management page include:

Attribute	Description
Username	<p>The username.</p> <p>Note</p> <p>Once a user group has been configured for a customer, the usernames of all end-users added at the relevant customer are automatically combined with the user group to create a unique user name, for example username@usergroup; where the username (in this field) is displayed adjacent to the user group (already configured by the System, Provider or Reseller administrator).</p>
Role	This indicates the users Role and cannot be modified.
Web service access	<p>Identifies the user's credentials for use by Web services API's, for example a 3rd Party system registering a phone.</p> <p>This is an optional field. Checkbox selected = Enabled (Web service access allowed), Checkbox not selected = disabled (not allowed).</p>
Security profile	The security profile related to the customer. Options include security profiles that have been configured for your system as well as the None and Default options.
Title	This is the title of the user, e.g. Mr, Mrs, Dr.
First name	This is the users first name. This is a mandatory field when either the conference or voicemail service is used.
Middle name	This is the users middle name, if applicable.
Last name	This is the Users last name. This is a mandatory field.
Contact telephone number	This is an alternate telephone number on which the user can be contacted.
Email address	<p>This is an email address for the user. This is a mandatory field when either the conference or voicemail service is used.</p> <p>Note</p> <p>When the end user is associated with a Webex conferencing service, this email address must be unique to the end user, i.e. not previously used by any other end user/username associated with a Webex conferencing service.</p>
Job title	This is the job title of the user.
Directory filter	Filter to be applied to the directory.
Information	Any important information relating to the user.
Misc	Miscellaneous data relating to the user.
Welcome message	The welcome message presented to the user when logging on.

Attribute	Description
Extra 1	Extra field for user data.
Extra 2	Extra field for user data.
Extra 3	Extra field for user data.
Extra 4	Extra field for user data.
GUI Branding	The branding theme to be presented to the user when they log into the system.
Preferred country	Displays the preferred country. Select from the drop-down list.
Override Language	The override language. Select from the drop-down list.
Access profile	Defines the menu options available to the user.
Account number to use in external accounting system	Account number if an external accounting system is being used.
Digest Credentials	Unified CM uses the digest credentials specified here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you associate the phone to the end user. Enter or edit a string of alphanumeric characters if required.
Confirm Digest Credentials	Re-enter the above credentials to confirm that you entered the digest credentials correctly.

Step 2 Click the **Modify** button at the bottom of the page. The selected user is modified in the system.

Administrator User Management

Users are divided into two key categories, End-users and Administrators.

- **Administrators:** An administrator at one level may only create other administrators at subordinate levels i.e. a Provider Administrator may not create other Provider Administrators, but may add Reseller, Customer and Location Administrators. Location Administrators may not create other Location Administrators or administrators on higher levels, and would therefore not have the option to add new administrator users. Administrator users are managed via the *General Administration > Administrator Users* menu.
- **End Users:** An end user is user of the service managed by the system. Typically telephony users may be either associated with a phone or be given an Extension Mobility profile. End users are managed via the *Location Administration > End Users* menu.

Note

This page outlines the management of Administrator Users, for information on managing end users please see the [Managing Users on page 839](#).

Procedure

Managing Administrator users

Note

An Administrator can only add a new administrator or modify an existing administrator at a level lower than his or her own level in the administration hierarchy.

To manage an Administrator User

- Step 1** Locate the user you want to manage and select the user by selecting the required *Username* (active text link).
- Step 2** Make the necessary modification to the User's details, or settings within the relevant boxes. For example, the User may have changed their job title or may require a new Feature Group.

Note

A red asterisk adjacent to a field indicates that it is a mandatory field.

The following fields are available when modifying a user:

Field	Description	Remarks
Username	The user who you are dealing with/modifying. This is a read-only field.	Note Once a user group has been configured for a customer, the usernames of all end-users added at the relevant customer are automatically combined with the user group to create a unique user name, for example username@usergroup; where the username (shown in this field) is displayed adjacent to the user group (already configured by the System, Provider or Reseller administrator).
Role	The type of user as defined when the user was created.	This is a read-only field.
Web service access	Identifies the user's credentials for use by Web services API's, for example a 3rd Party system registering a phone.	This is an optional field. Checkbox selected = Enabled (Web service access allowed), Checkbox not selected = disabled (not allowed).
Security profile	The security profile related to the customer. Options include security profiles that have been configured for your system as well as the None and Default options.	-
Title	Title of user	-
First name	First Name of user.	This is a mandatory field when either the conference or voicemail service is used.
Middle name	Middle name of user.	-
Last name *	Last name (surname) of user.	This is a mandatory field. Sometimes referred to as "Surname".
Home telephone number	Home telephone number of user.	-
Mobile telephone number	Mobile phone number of user.	-
Contact telephone number	Contact telephone number of user.	-

Field	Description	Remarks
Alternative telephone number	Alternate contact number for user.	-
Email address	User email address.	<p>This is a mandatory field when either the conference or voicemail service is used.</p> <p>Note</p> <p>When the end user is associated with a Webex conferencing service, this email address must be unique to the end user, i.e. not previously used by any other end user/username associated with a Webex conferencing service.</p>
Job title	Job title of user.	-
Directory filter	-	-
Information	-	-
Misc	-	-
Welcome message	-	-
Extra 1	-	-
Extra 2	-	-
Extra 3	-	-
Extra 4	-	-
Department	Department of user	-
Department Code	Department Code of user	-
GUI Branding	The branding theme (colors, fonts, items look & feel etc) to be presented to the user when they log in.	<p>Select from the drop-down list.</p> <p>The themes (branding) are defined by the Provider administrator. The applicable themes should be enabled for each level in the hierarchy.</p>
Access Profile	Defines menu options available for the user.	<p>Select from a drop-down list.</p> <p>The available access profiles are defined by the Provider Administrator. The default access profile is provided as part of the product.</p>
Account number to use in external accounting system	-	-
Digest Credentials	Enter a string of alphanumeric characters.	<p>Unified CM uses the digest credentials specified here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you associate the phone to the end user.</p>

Field	Description	Remarks
Confirm Digest Credentials	Re-enter the above credentials to confirm that you entered the digest credentials correctly.	-

- Step 3** Click the **Modify** button at the bottom left hand corner of the screen when complete. The admin users details are updated.

Managing Numbers

This section covers the location administration process for managing peripheral services and information. These are:

- Telephony
- Number Groups
- Pickup Groups
- Hunt Groups

Telephony Management

This section covers the process for managing telephone numbers within the system, including both external and internal numbers. As an Operator, you are required to process telephone numbers and so need to understand this number management process. From this page, you are able to access:

For information on the SBC functionality, see [Session Border Controller Management \(SBC\) on page 453](#).

Note

Depending on the configuration of your system, available options may differ.

- **Telephony** - Select this button to facilitate the connection and disconnection from the PSTN. See [Connect to a PSTN on page 886](#).
- *Call Park* - Select this active text link to manage the call park feature. This provides users with, amongst other things, the ability to place a call on hold, so it can be retrieved from another phone. See [Call Park on page 887](#)
- *Directed Call Park* - Select this active text link to manage the directed call park feature. This allows users with, amongst other things, the ability to park a call against their own Directory Number or to direct the call to be parked against another directory number in their assigned group. See [Add a Directed Call Park on page 891](#)
- *Gateways* - Select this active text link to manage the Local and SRST Gateways. See [Local / SRST Gateway Management on page 885](#)
- *CTI Management* - Select this active text link to manage the CTI Route points and ports. See [CTI/TAPI Management on page 442](#)
- *Meet-Me* - Select this active text link to manage the MeetMe Conferencing feature. See [Meet-Me on page 376](#)
- *Device Pool* - Select this active text link to manage device pools at location level. See [Device Pool Management on page 894](#)
- *Presence Monitoring* - Select this active text link to manage presence monitoring at location level. See [Presence Monitoring on page 910](#)

- *Emergency Response Location Management* - Select this active text link to manage the emergency call feature. See [Emergency Response Location Management on page 893](#)
- *Location Unmanaged Legacy Gateways* - Select this active text link to enable an administrator to activate the ports for Legacy Gateways at an unmanaged location. See [Legacy Gateway Dial Plan Provisioning on page 897](#)

Local / SRST Gateway Management

To access the *Local Gateway Dial Plan Provisioning* screen:

Procedure

Step 1 Browse to *Location Administration > Telephony*.

Step 2 Select the *Gateways* active text link.

The resultant screen displays a list of activated and deactivated gateways. From this screen you are able to:

- Deactivate activated gateways
- Activate deactivated gateways
- Delete dial plans
- Modify Dial Plans
- Manage Call Routing

Procedure

Activating a Gateway Port

Note

Once a port has been activated at a location it cannot be reconfigured. Such ports must first be deactivated at the location before they can be reconfigured.

To activate a gateway port:

Step 1 Browse to the *Local Gateway Dial Plan Provisioning* screen using the instructions above.

Step 2 Select the checkboxes adjacent to the gateway ports that you would like to activate.

Step 3 Click the **Activate** button when complete. The selected gateway ports are activated.

Procedure

Deactivating a Gateway Port

To deactivate a gateway port:

Step 1 Browse to the *Local Gateway Dial Plan Provisioning* screen using the instructions above.

Step 2 Select the checkboxes adjacent to the gateway ports that you would like to deactivate.

Step 3 Click the **Deactivate** button when complete. The selected gateway ports are deactivated.

Procedure

Deleting Dial Plans

To delete a dial plan:

- Step 1** Browse to the *Local Gateway Dial Plan Provisioning* screen using the instructions above.
- Step 2** Click the **Delete Dial Plan** button. The dial plan is deleted.
-

Procedure

Modifying a Dial Plan

To modify a dial plan:

- Step 1** Browse to the *Local Gateway Dial Plan Provisioning* screen using the instructions above.
- Step 2** Click the **Modify Dial Plan** button.
- Step 3** Make the required modifications and click the **Modify** button. The dial plan is updated with your modifications.
-

Procedure

Modifying Call Routing

To modify Call Routing:

- Step 1** Browse to the *Local Gateway Dial Plan Provisioning* screen using the instructions above.
- Step 2** Click the **Call Routing** button.
- Step 3** Make the required changes to call routing then click the **Modify** or **Submit** button as appropriate. The Call Routing is updated.
-

The Gateway Call Routing page is divided into two sections, one for Location level call routing and the other for Local Gateway Port Call Routing. On this page is a list of all the call types associated to the country of the location. Radio buttons adjacent to each call enables you to select between Local and Central call paths. The Local Gateway Port call routing section is only displayed when location level call routing has been configured and the H323 ports have been activated at the location. The *Apply Configuration To Trunks* Settings are only displayed if H323 ports have been activated at the location and the location call routing has been applied. Two options are displayed for this setting *Once for all Call Types* and *Once Per Call Type*. If *Once for all Call Types* is selected, then IOS model are applied per trunk for all the call types, if *Once Per Call Type* is selected, the model is applied once per trunk per call type. By default, the *Once for all Call Types will be displayed*. Once the port call routing has been applied using this setting, the drop-down list is disabled.

Connect to a PSTN

This functionality is primarily used for roll-out or migration of new users. It allows administrators to plan and prepare a location with new (or migrated) users including some tests in advance without having to rush it in the "go live" day.

This function allows for all the provisioning steps for a location, leaving only the last step of connectivity of the live PSTN lines to this location, as a last minute activity.

This speeds up the live roll-out / migration and helps minimize the provisioning issues and mistakes at the critical time.

Note

- When deploying a new location, it is good practice to first verify all the IP phones work with calls within the location, assign all the DDI's, hunt groups etc, and if everything is working fine, then 'Connect' to the PSTN as the last step.
- This functionality is model driven, so which components you alter or leave out of the dial plan, is completely flexible. When you are ready to have the new site go live, you click the **Connect** button; this calls whatever is specified in the model, and completes your dial plan.

Procedure

To connect or disconnect to the PSTN:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Click the **Telephony** button.
- Step 3** Click the **Connect** button.
-

See also:

- [Adding a Phone to the Phone Inventory on page 834](#)
 - [Adding a location on page 749](#)
-

Call Park

The Call Park feature enables users to place a call on hold and then retrieve it from another phone.

There are two types of call parks:

- Standard
- Directed

The Standard Call Park feature enables users to place a call on hold so that it can be retrieved from another phone in the system (for example, a phone in another office or in a conference room). If users are on an active call, they can park the call to a call park extension by pressing the **Park** soft key or the **Call Park** button. Someone on another phone in the system can then dial the call park extension to retrieve the call.

Users can define either a single directory number or a range of directory numbers for use as call park extension numbers. Users can park only one call at each call park extension number.

The *Directed Call Park* feature is a special form of hold that allows users to park a call against their own Directory Number or to direct the call to be parked against another directory number in their assigned group.

The user who parked the call (or another party) can then retrieve the call from the same phone or from a different phone in the same group. The parked party perceives that the call has been placed on hold.

Note

Within linked locations, parent and child locations share Call Park ranges. It does not matter if the ranges are created at the parent or the child location, all

locations that are part of the linked location setup use the extension pool. Hence, parked call retrieval is possible across linked locations.

Call Park Prefixes

To distinguish between Call Park numbers internally, the system uses a custom prefix, followed by a number increment, one per call processing server in a Location's Cisco Unified Communications Manager (Unified CM) group. The Prefix can be set by the system administrator, either at the System level, where it applies to all Locations (as a default,) or at the individual Location level. It can contain the characters #,* or 0-9, and the existing dial plan should be taken into consideration when assigning it.

As the Prefix is common to all Call Park internal numbers in a Location, the system uses a Sequence Number to ensure that all Call Park numbers are unique in a cluster. Call Park numbers are only created on Unified CM servers marked as Call Processor Engines (CPEs.) For each additional CPE that is targeted during the Call Park create sequence, the Internal Sequence Number portion of the Call Park identifier is incremented by one. This Number is a two digit number starting at 01.

The format of the Internal Call Park number is *%Prefix%SequenceNo%DN*. The remaining DN portion of the Call Park number is a range of numbers, based on the number of Call Park DNs required:

- "00" is the single starting DN if only one Call Park is chosen
- "00" to "09" is the starting range of DNs if a 10 Call Park range is chosen
- "00" to "99" is the range of DNs if a 100 Call Park range is chosen

If an administrator selects #2 as a Call Park Prefix and creates a 10 number Call Park range, the numbers would be #20100, #20101 etc. on Server A and #20200, #20201 etc. on Server B. When a user parks a call, the correct number is displayed and the second user collecting the call can successfully retrieve it from the uniquely numbered destination.

Updating the Call Park Prefix

Procedure

To specify the Call Park Prefix:

- Step 1** Browse to *Dial Plan Tools > Number Construction*.
- Step 2** Select the *Name* (active text link) of the required dial plan.
- Step 3** Specify the required Call Park Prefix in the Call Park Prefix field.
- Note:** This field can contain the characters #,* or 0-9.
- Step 4** Click the **Modify** button. The call park prefix is updated.
-

Note

The call park prefix can also be updated via the bulk loaders.

Location Call Park

The Call Park feature enables you to place a call on hold so that it can be retrieved from another phone in the system (for example, a phone in another office or in a conference room). If you are

on an active call, you can park the call to a call park extension by pressing the **Park** soft key or the **Call Park** button. Someone using another phone in your system can then dial the call park extension to retrieve the call. You can define either a single directory number or a range of directory numbers for use as call park extension numbers.

Notes:

- You can only park one call at each call park extension number.
- Within linked locations, parent and child locations share Call Park ranges. It does not matter if the ranges are created at the parent or the child location, all locations that are part of the linked location setup will use the extension pool. Hence, parked call retrieval is possible across linked locations.
- Before adding a call park, please ensure that you have configured a Call Park prefix within the dial plan.

Procedure

Managing a Call Park

Follow these steps to modify a call park :

Step 1 Browse to *Location Administration > Telephony > Call Park*

Step 2 Select the **Call Park** (active text link) that you wish to delete

To delete call park ranges, select the checkboxes adjacent to the required call park ranges then select the **Delete** button.

To add a call park range, select the required range size from the drop-down list then select the **Add** button.

The relevant changes will be applied to the Call Park

The following fields are displayed when managing a call park, but cannot be modified on this page:

Field	Description
<i>Name</i>	A unique name for the directed call park number or range
<i>Description</i>	A brief description of this directed call park number or range
<i>Call Park Prefix</i>	This is the Call park prefix that is configured in the relevant dial plan. This field cannot be edited on this page unless the <i>Call Park Location Configurable?</i> option is selected in the active dial plan. If the <i>Call Park Location Configurable?</i> option is active, the Call park prefix can be specified when adding a call park.
<i>Call Park Range Size</i>	Select the required call park range from the drop-down list. Options include 1, 10 and 100.

Procedure

Delete a Call Park

Follow these steps:

Step 1 Browse to *Location Administration > Telephony > Call Park*

- Step 2** Select the **Call Park** that you wish to delete
- Step 3** Select the checkboxes adjacent to all call park ranges then select the **Delete** button.
-

The call park will be deleted from the system.

Modify Directed Call Park

Procedure

To modify a Call Park:

- Step 1** Modify the required fields
- Note:** You can create a maximum of 100 call park numbers with one call park range definition. The call park numbers need to be unique.
- Step 2** Select the **Modify** button
-

The following fields are available:

Field	Description
<i>Name</i>	A unique name for the directed call park number or range
<i>Description</i>	A brief description of this directed call park number or range
<i>Call Park Range Start</i>	Start number of the defined range of the directed call park numbers
<i>Call Park Range End</i>	End number of the defined range of the directed call park numbers
<i>Reversion Number</i>	The Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, the system generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.
<i>Reversion Class of Service</i>	Class of Service
<i>Retrieval Prefix</i>	For this required field, enter the prefix for retrieving a parked call. The system needs the retrieval prefix to distinguish between an attempt to retrieve a parked call and an attempt to initiate a directed park.

Add a Standard Call Park

Note

You can create a maximum of 100 call park numbers with one call Park Range definition.

Procedure

To add a Standard Call Park:

- Step 1** Browse to *Location Administration > Telephony > CallPark*.
- Step 2** Click the **Add** button.
- Step 3** Enter the name and description of the call park.

- Step 4** If required, update the Call Park prefix.
- Step 5** Select the required Range Size from the drop-down list then click the **Submit** button.

Procedure

Add a Call Park Range to a Standard Call Park

To add a Standard Call Park Range:

- Step 1** Browse to *Location Administration > Telephony > CallPark*.
- Step 2** Select the name of the Call Park you wish to modify.
- Step 3** Select the required range size from the drop-down list then click the **Add** button. The call park range is added.

Procedure

Delete a Call Park

To delete a Call Park Range:

- Step 1** Browse to *Location Administration > Telephony > CallPark*.
- Step 2** Select the name of the Call Park you wish to modify.
- Step 3** Select the checkbox(es) of all Call Park Ranges that you want to delete, and then click the **Delete** button. The selected call park ranges are deleted.

Add a Directed Call Park

Procedure

To add a Directed Call Park:

- Step 1** From the menu, select *Location Administration > Telephony > Directed CallPark*.
- Step 2** Click the **Add** button.
- Step 3** Enter details as required and click the **Submit** button.

Note

You can create a maximum of 100 call park numbers with one call Park Range definition. Make sure the call park numbers are unique.

The following table refers to the above:

Field	Description	Remarks
Name	A unique name for the directed call park number or range.	This is a mandatory field.

Field	Description	Remarks
Description	A brief description of this directed call park number or range.	-
Call Park Range Start	Start number of the defined range of the directed call park numbers.	Make sure that the directed call park numbers are unique and that they do not overlap with other call park numbers.
Call Park Range End	End number of the defined range of the directed call park numbers.	-
Reversion Number	The Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, the system generates alerts, such as a ring or beep, to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.	-
Reversion Class of Service	Class of Service	-
Retrieval Prefix	For this required field, enter the prefix for retrieving a parked call. The system needs the retrieval prefix to distinguish between an attempt to retrieve a parked call and an attempt to initiate a directed park.	This is a mandatory field.

Delete Directed Call Park

Procedure

To Delete Directed Call Park:

From the menu, browse to *Location Administration > Telephony > Directed Call Park*.

Step 1 Select the *Directed Call Park* or range of numbers you wish to delete.

Step 2 Click the **Delete** button.

Note

Deleting a directed call park number causes the system to immediately revert any call that is parked on that number.

Model Based Call Parks

The system has a provision to add Call Park numbers specified in the Cisco Unified Communications Manager (Unified CM) model loaders at the time of initializing the Unified CM cluster. The database table used to store model based Call Park numbers is *ccm4_1_3_model_callpark*. The settings stored in this table are call park name, call park pattern, call park partition, dialplan name, template name, description, site specific. The values of site specific and transaction type should be set as *N* and *InitIPPBX* respectively for the call park numbers to be added at the time of initializing the Unified CM cluster.

The call park numbers are added on each of the servers available in Unified CM cluster being initialized. The call park numbers are added in the same partition on the Unified CM but include a unique subscriber sequence. The call park pattern includes a variable `#CCMSUBSCRIBERSEQ#`, which is replaced with a count of the Unified CM servers in the Unified CM group.

Emergency Response Location Management

Correctly configured emergency numbers ensure that emergency calls are routed to the appropriate public safety answering point (PSAP) for the caller's location and that the PSAP can identify the caller's location and return the call if necessary.

Procedure

Adding an Emergency Response Location

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *Emergency Response Location Management* (active text link).
- Step 3** Click the **Add** button.
- Step 4** Complete the required fields then click the **Submit** button.

The emergency response location is added to the location.

The following fields are available when adding an emergency response location:

Field	Description
<i>Name</i>	The name of the emergency response location being added. This is a mandatory field.
<i>Description</i>	A short description of the emergency response location being added.
<i>Emergency Hardware Group</i>	Select the hardware group that contains the emergency server that you would like to use. This is a mandatory field.

Procedure

Modifying an Emergency Response Location

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *Emergency Response Location Management* (active text link).
- Step 3** Select the *Name* (active text link) of the emergency response location management that you would like to modify.
- Step 4** Modify the required fields then click the **Modify** button.

The emergency response location is modified.

Procedure

Deleting an Emergency Response Location

- Step 1** Browse to *Location Administration > Telephony*.

- Step 2** Select the *Emergency Response Location Management* (active text link).
- Step 3** Select the *Name* (active text link) of the emergency response location management that you would like to delete.
- Step 4** Click the **Delete** button.

The emergency response location is deleted.

Important

Depending on the configuration of your system, confirmation may not be requested when deleting emergency response locations.

Procedure

Adding an Emergency Location Identification Number (ELIN)

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *Emergency Response Location Management* (active text link).
- Step 3** Select the *Name* (active text link) of the emergency response location management that you would like to modify.
- Step 4** Click the **Add ELIN** button.
- Step 5** Select the required ELIN from the drop-down list then click the **Add** button.

The ELIN is added.

Procedure

Deleting an ELIN

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *Emergency Response Location Management* (active text link).
- Step 3** Select the *Name* (active text link) of the emergency response location management that you would like to modify.
- Step 4** Click the **Delete** button adjacent to the ELIN that you would like to delete.

The ELIN is deleted.

Device Pool Management

Device pools make common Cisco Unified Communication Manager (Unified CM) resources and settings available to devices using these device pools. Multiple device pools at a location provides administrators more flexibility by allowing them to separate these resources logically and/or more efficiently. Device pools include elements such as which Unified CM group to use, and which Region to use (determines bit rates/codecs).

Previously, when adding a location, a device pool was created for the location using a set of pre-determined (hard-coded) values. SRST was implemented for a location by making a copy of the hard-coded device pool with slightly adjusted settings. The new device pool functionality allows

users to continue as they have before, using a 'typical' configuration for the device pool when adding a location, but also provides them with the ability to customise device pools for improved device pool management.

Users can now control and configure a selected set of device pool settings, which allows them to both specify these settings for the device pool when adding the location, and to modify these settings after the device pool has been created. In addition, it allows administrators to create additional device pools for a location after the location has been added (one device pool created when adding the location), and to subsequently assign specific devices to specific device pools in order to better control the usage and setting of specific devices. If for example a user wants to use two different sets of audio codecs in a location, or use a different Unified CM group for certain devices, then two separate device pools can be created, each containing the relevant devices. SRST device pool management has also been enhanced in a similar way, allowing various settings to be set and managed by the administrator.

Even though Unified CM does not specifically distinguish between device pools based on any specific type, CUCDM provides a logical typing to better manage/control the various device pools based on their specific purpose. CUCDM distinguishes between the following device pool types:

- **Location:** This type of device pool gets created when adding a location or when adding an additional device pool at a location.
- **SRST:** This type of device pool gets created with an SRST reference, and is also available for use at location.
- **EMCC and system:** These device pools are managed via the specific feature screens, and not via the device pool management functionality at the location.

There is no device pool management for unmanaged locations, where the device pool used is determined during the creation of the unmanaged location.

Every location must have at least one device pool, which must be set as the 'Default'. The default device pool must be of type 'Location', and is used during MACToLocation, AutoRegister and AutoMoveToLocation. Device pools created as part of the location before the introduction of this feature are migrated as the default for the location.

SRST handling has changed significantly to support an environment where locations have multiple device pools. Previously, a LBO Gateway was required before an SRST reference was added, that is, ports had to be configured on the gateway before SRST configuration could be completed. These two functions are now separate, effectively allowing the customer to add a SRST role to an IOS device without having to configure the LBO (Gateway Role) first. Note however that the Gateway Role and configuration is still required in order for the IOS Device to function correctly.

If a phone does not have SRST enabled in its feature group, then only device pools of type 'Location' are available to assign to the device. If a phone has SRST enabled in its feature group, then there is a checkbox to 'Enable SRST'. This exposes the list of SRST references for that location, each displaying the remaining capacity as per current functionality, and the list of available device pools is filtered based on the SRST reference chosen.

A Unified CM cluster's capacity is determined by a number of streams. These are consumed by Unified CM groups, which are referenced in device pools. The sum of the supported streams for all the device pools using the same Unified CM group may not exceed the number of streams allocated to the Unified CM group. This validation is only done when creating the device pool and no counting of devices assigned to any specific device pool is enforced.

All Device pools created by the Cisco Unified Communications Domain Manager (CUCDM) on the Location level are displayed on the *Device Pool Management* screen. These include *Location* and/or *SRST* type device pools. Device pools automatically created during specific feature provisioning workflows not directly related to the location, such as EMCC roaming device pools, are not listed on this page, and can not be managed at the location.

Note

One of the device pools at a location must be configured as the 'default' device pool. The default device pool is used during MACToLocation, AutoRegister and AutoMoveToLocation. The default device pool can be changed at any time by modifying the specific device pool and selecting (enabling) the *Default Device Pool* checkbox.

Procedure

To access the Device Pool Management screen:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Click the **Device Pool** button. The *Device Pool Management* screen is displayed.
-

This screen allows a location administrator to view existing device pools at a location, add new device pools to a location, modify existing device pools in a location, or delete device pools from a location.

Adding a Device Pool

Procedure

To add a device pool:

Note

A device pool can not be added without a device pool template.

- Step 1** Click the **Add** button on the *Device Pool Management* screen. The *Add Device Pool* screen is displayed.
- Step 2** Complete the required fields (see [Add Location - Page 3 on page 753](#) under Device Pool/Configuration/Custom). Edit the relevant pre-populated fields if required.
- Step 3** Click the **Add** button when complete to add the device pool to the location.
-

Modifying a Device Pool

Procedure

Warning

When you modify a device pool, a soft reset (restart) is performed on all devices associated with the device pool. This may be disruptive to users.

To modify an existing device pool:

- Step 1** Click the relevant device pool *Name* (active text link) that you want to modify. The *Modify Device Pool* screen is displayed.
- Step 2** **Note**
- Device pool types cannot be modified, for example a "Location" type cannot be changed to "SRST" type.

Edit the fields as required (see [Add Location - Page 3 on page 753](#) under Device Pool/Configuration/Custom).

- Step 3** Click the **Modify and Reset** button when complete to save the changes to the device pool at the location.

Note

The default device pool can **not** be deleted.

To delete a device pool, click the **Delete** button on the appropriate *Modify Device Pool* screen.

Legacy Gateway Dial Plan Provisioning

Procedure

Location Unmanaged Legacy Gateways

To activate allocated legacy gateway ports at the location:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select *Location Unmanaged Legacy Gateways* (active text link).
- Step 3** Select the ports to activate for the relevant deactivated Gateway.
- Step 4** Click the **Activate** button.
- Step 5** On the next screen, a *Calling Search Space (CSS)* text field is displayed, with a default value populated from the loaded HCS model.
- Leave this value as the default or change it to the appropriate CSS value.
- Step 6** Specify the *Call Agent Order* by selecting a port from the list and then moving its position in the order up or down by selecting the up or down buttons.
- Step 7** Click the **Add** button.

Note

When activating the ports, the IPPBX selected at Gateway configuration is provisioned with the Route Lists, Route Groups and Route Patterns configured in the loaded HCS model. The *AddLocationLegacyGateway* transaction uses the *#LOCATION-ID#* variable.

Number Group Management

A Number Group is a set or group of phones that can be used by one or multiple Hunt Groups in a Hunt Group List. Organizations utilize Number Groups to ensure that calls to their employees can be answered promptly with minimal effort.

Note

A number group must be selected by a Hunt Group, otherwise it performs no function.

To manage your number groups:

Select the *Number Groups* option from the *Location Administration* menu.

Create Number Groups

Procedure

To create a number group:

- Step 1** Click the **Add** button on the *Number Group Management* screen. The *Add Number Group* screen is displayed.
- Step 2** Complete the required fields (see table below), clicking the **Next** button when required:

Field	Description	Remarks
Name	A unique name for the Number Group. This is a mandatory field.	-
Description	A brief description of the Number Group.	-
Device Group	The selected device group.	This is an optional field. Select the required device group from the drop-down list.
Hunt On Busy	Performs the selected behavior when the number is busy.	Select from the drop-down list. <i>Stop hunting:</i> If you select this hunt option, the system stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call. <i>Try next member, then, try next group in Hunt List:</i> If you select this hunt option, the system distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, the system then tries the next line group in a hunt list. <i>Skip remaining members, and go directly to next group:</i> If you select this hunt option, the system skips the remaining members of this line group upon encountering a busy member; the system proceeds directly to the next line group in a hunt list. <i>Try next member but do not go to next group:</i> If you select this hunt option, the system distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. The system stops trying upon reaching the last member of the current line group.
Hunt No Answer	Performs a selected behavior when the number is busy.	Select from the drop-down list (as described above).

Field	Description	Remarks
Automatically Logout Hunt Member on No Answer	<p>Select (enable) checkbox if required.</p> <p>Note</p> <p>This field is only available in Unified CM version 9.1.1 and higher.</p>	<p>If selected, line members who do not answer are logged off the hunt list automatically. Line members can log back in using the "HLOG" softkey or PLK.</p> <p>See also Adding a Hunt Group on page 902.</p>
Hunt Not Available	Performs a selected behavior when the number is busy.	Select from the drop-down list (as described above).
Distribution Method	This determines the order in which the numbers within the number list are called when a call is directed to the pilot number assigned to the hunt group that uses this number group.	<p>Select from the drop-down list.</p> <p>Longest Idle time:</p> <p>If you select this option, the system only distributes a call to idle members, starting from the longest idle member to the least idle member of a line group. This feature evenly distributes the incoming call load among the members of the hunt group.</p> <p>Circular:</p> <p>This feature maintains a record of the last hunt group member to receive a call. When a new call arrives, the system routes the call to the next hunt group member in the hunt group.</p> <p>Top Down:</p> <p>If you select this option, the system distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Broadcast:</p> <p>If you select this option, the system distributes a call to all idle or available members of a line group simultaneously.</p>
RNA Reversion Timeout	The time, in seconds, after which the system distributes a call to the next available or idle member of a line group or, to the next line group if the call is not answered, and if the first hunt option, Try next member; then, try next group in Hunt List, is chosen.	<p>Select from the drop-down list.</p> <p>The RNA Reversion Timeout applies at the line-group level to all members. This value should be configured short enough to allow each number to be called before the Maximum Hunt Timer, specified in any associated Hunt Group, expires. The maximum length of time that can be set for this timer is 180 seconds (3 minutes).</p>
Line Number	The number that allows the group to be addressed by phones that are not in the group.	Select from the drop-down list.

Step 3 Click the **Add** button when complete to add the number group to the system.

Modify a Number Group

Procedure

To modify a number group:

- Step 1** Select the Number Group *Name* (active text link) on the *Number Group Management* screen of the Number Group that you wish to manage. The *Manage Number Group* screen is displayed.
- Step 2** Change the required fields and click the **Modify** button. For an explanation of the fields, see [Create Number Groups on page 898](#).
-

Add a number to a number group

Procedure

To add a number to a number group:

- Step 1** Select the *Name* (active text link) on the *Number Group Management* screen of the Number Group that you wish to manage. The *Manage Number Group* screen is displayed.
- Step 2** Click the **Add Number** button to add a number. The *Add Number* screen is displayed.
- Step 3** Select a number to add to the Number Group from the drop-down menu.
- Step 4** Click the **Add** button. The number is added to the Number Group.
-

Note

You can add several numbers at the same time by using CTRL + Select when you select the numbers to add.

Delete number from a Number Group

Procedure

To delete a number from a number group:

- Step 1** From the *Manage Number Group* screen, you can see the list of numbers within the group.
- Step 2** Click the **Delete Number** button adjacent to the number that you wish to remove from the Number Group. The system automatically removes the number from the Number Group.
-

Note

You can delete several numbers at the same time by clicking the delete button one after the other without waiting for the system transaction to complete. The system queues the delete transactions and performs all of them once you are complete, preventing you having to return to the screen for the next number delete.

Reorder Numbers in a Number Group

When a call in a selected Hunt Group is received the Hunt List has an order to determine which number group is called first. The re-order tab is used to change the order of the number groups to be answered.

Procedure

To Reorder Numbers in a Number Group:

- Step 1** From the *Manage Number Group* screen, select the Number Group you want to edit - this displays the details below.

- Step 2** Click the **Re-order** button.
- Step 3** Select the relevant number you want to edit, and then click the **Move Up/Move Down** buttons as required.
- Step 4** Click the **Update** button when complete to save the changes.

Delete a Number Group

To delete the Number Group, you must delete all the numbers first.

Procedure

- Step 1** From the **Manage Number Group** screen, select the name of *Number Group* that you want to delete.
- Step 2** On the *Manage Number Group* screen, click the **Delete** button at the bottom right hand corner relevant to the number group that you wish to remove.

Hunt Group Management

A hunt group is a set of phones to which rules can be applied so that calls can be answered more efficiently. Depending on the rules, a call to any phone in the group causes all the phones to ring at the same time, or each phone rings in turn and the call is forwarded to the next phone in the group until it is answered.

Hunt Groups utilize Number Groups. Therefore, in order to create or manage Hunt Groups, the relevant Number Groups must be available in the location.

See also: [Number Group Management on page 897](#).

[Adding a Hunt Group on page 902](#)

Procedure

Deleting a Hunt Group

To delete a Hunt Group:

- Step 1** Select the required hunt group *Name* (active text link) on the *Hunt Group Management* screen that you wish to delete.
- Step 2** Click the **Delete** button. The hunt group is removed from the system.

[Modifying a Hunt Group on page 905](#)

Managing Number Groups in a Hunt Group

Hunt Groups are configured by allocating Number Groups to them. The allocation and order of these number groups determines the order and method in which the phones in the hunt group ring.

The hunt group forwards the call to the first number group in the list of associated number groups. A number group can be configured to forward the call to another number group when it is not answered in a specified length of time. This option determines the order in which each number group is called.

Therefore, having available Number Groups in the location is a prerequisite for using Hunt Groups.

Procedure

To manage number groups within a Hunt Group:

- Select the hunt group *Name* (active text link) on the *Hunt Group Management* screen that you want to manage.
-

Note

By selecting the Number Group name, you can manage the number group itself. Further details are available under [Hunt Group Management on page 901](#).

Procedure

Add / Connect a Number Group to a Hunt Group

To add a new Number Group to an existing Hunt Group, complete the following steps, after you have chosen the Hunt Group you want to manage:

- Step 1** Click the **Select Number Group** button on the *Hunt Groups Management* screen. The Select Line Group screen is displayed.
- Step 2** Select the order in which the new Number Group is called by the Hunt Group via the drop-down selection list.

Note

The order in which you define the number groups does not have to be consecutive. However the Hunt Group use of the number groups is in ascending order.

- Step 3** Select the Number Group to add to the Hunt Group from the drop-down list, and then click the **Submit** button.
-

Note

- The list shows the available Number Groups in the location which are not yet associated with this Hunt Group.
 - A Number Group can be associated with multiple Hunt Groups.
-

Procedure

Delete / Disconnect a Number Group from a Hunt Group

- Step 1** You cannot change the order of number groups in a hunt group, so you must disconnect the number group from the hunt group by clicking the *Disconnect Number Group* button adjacent to the relevant number group.
- Step 2** Re-add it in the correct, required, order.
-

Adding a Hunt Group

Procedure

Adding a Hunt Group

To create a Hunt Group:

Step 1 Click the **Add** button on the *Hunt Group Management* screen.

Step 2 Enter the required fields. The available fields include:

Field	Description	Remarks
Details		
Name	Provide a name for the Hunt Group.	This is a mandatory field.
Description	Provide a brief description of this Hunt Group.	-
Device Group (Tenant)	Select the required device group from the drop-down list.	This is an optional field.
Pilot Number	A pilot number is a virtual directory number that is never busy. It alerts the system to receive and direct calls to hunt group members. A hunt group comprises a list of destinations that determine the call redirection order.	This is a mandatory field. Select from the drop-down list.
Number Group Name	Before you can add a Hunt group, you must first create the number group - Select the relevant Number Group from the drop-down list.	This is a mandatory field. Select from the drop-down list.
Ex Directory	If selected the number is excluded from the Corporate Directory list.	Disable the checkbox (default) - the feature is off. Enable the checkbox to turn feature on.
Hunt Pilot Configuration		
Maximum Hunt Timer (seconds)	This Timer specifies the total length of time that the incoming call rings on any associated number groups before it is forwarded to the number specified in the Call Forward Destination field.	This value is presented in the form of seconds. This field may only contain numeric characters and is limited to values between 1 and 3600.
Call Pickup Group	Lists all the Call Pickup Groups that are available in the same location as the hunt group being added.	Select the required Call Pickup Group from the drop-down list, default = None. The Hunt Group Pilot number is added to the selected Call Pickup Group.
Hunt Forward Settings		
Select the <i>Hunt Forward Settings</i> radio button to enable/configure the required forward hunt preferences (see below).		
Note <i>Hunt Forward Settings</i> and <i>Call Queueing</i> are mutually exclusive, that is only one of the options can be selected.		
Use Personal Preferences?/Forward Hunt No Answer	Allows you to select the status of the <i>Forward Hunt No Answer</i> personal preference setting.	Checkbox selected = setting enabled, checkbox not selected = setting disabled.
Use Personal Preferences?/Forward Hunt Busy	Allows you to select the status of the <i>Forward Hunt Busy</i> personal preference setting.	Checkbox selected = setting enabled, checkbox not selected = setting disabled.

Field	Description	Remarks
Class of Service	The Class of Service (CoS) lists adjacent to each Hunt Forward setting display a list of the valid forward CoS types in the Cisco Unified Communications Domain Manager (CUCDM).	<p>Select the required CoS settings from the drop-down list for each Hunt Forward setting.</p> <p>Class of Service (CoS) to Calling Search Space (CSS) mappings exist in the Cisco Unified Communications Domain Manager (CUCDM) models. Selecting a CoS provisions its corresponding CSS on Cisco Unified Communications Manager (Unified CM). By default, the CoS that is set in the 'HuntGroup-CallFwdCOS' customer preference is pre-selected. Selecting 'Default CoS' for a Hunt Forward Setting results in the CSS that is mapped to the CoS set in the 'HuntGroup-CallFwdCOS' customer preference being provisioned to the Unified CM. If the customer preference is set to 'Default CoS', the CSS is provisioned based on the global call forward CSS name that is derived from the dial plan models. If the CoS in the customer preference is changed, the CoS for Hunt Forward Settings that are set to 'Default CoS' are not automatically updated to the new CoS.</p>
<p>Queue Calls</p> <p>Select the <i>Queue Calls</i> radio button to enable/configure the required queue call preferences (see below).</p> <p>Note</p> <p>This option is available only to location (or higher) administrator's to configure Call queueing parameters (for Unified CM version 9.1.0 and above only).</p>		
Network Hold MOH Source & Announcements	Determines the music on hold/announcement options.	<p>Select from the drop-down list.</p> <p>Note</p> <p>Custom announcements and MoH must already be uploaded/configured in Unified CM, and the required MoH track must be available in CUCDM.</p>

Field	Description	Remarks
Maximum Number of Callers Allowed in Queue	This is a mandatory field. Enter the required maximum number of callers allowed in the queue (1 to 100 - default = 32).	Select the required action (radio button) to perform when the queue is full, that is <i>Disconnect the call</i> or <i>Route the call to this destination</i> . Enter the required destination to which to route the call (mandatory if selected), and then select the required <i>Full Queue Class of Service (CoS)</i> from the drop-down list.
Maximum Wait Time in Queue	This is a mandatory field and determines the maximum wait time in the queue (in seconds).	Enter the required maximum wait time (10 to 3600 seconds - default = 900).
When Maximum Wait Time is Met	Determines the action to perform when the maximum wait time (see above) has elapsed.	Select the required action (radio button) to perform when the selected maximum wait time in queue has elapsed, that is <i>Disconnect the call</i> or <i>Route the call to this destination</i> . Enter the required destination to which to route the call (mandatory if selected), and then select the required <i>Max Wait Time Class of Service (CoS)</i> from the drop-down list.
When no hunt members answer, are logged in, or registered	Determines the action to perform when no hunt members answer, are logged in, or registered.	Select the required action (radio button) to perform when no hunt members answer, are logged in, or registered, that is <i>Disconnect the call</i> or <i>Route the call to this destination</i> . Enter the required destination to which to route the call (mandatory if selected), and then select the required <i>No hunt members logged in or registered (CoS)</i> from the drop-down list.

Step 3 Click the **Add** button when complete. The hunt group is added to the system.

Modifying a Hunt Group

Procedure

Modifying a Hunt Group

To modify a Hunt Group:

- Step 1** Select the required hunt group *Name* (active text link) on the *Hunt Group Management* screen that you want to modify.
- Step 2** Edit the fields as required and click the **Modify** button when complete. For an explanation of available fields, see [Adding a Hunt Group on page 902](#).

Pickup Groups

Call Pickup and Group Call Pickup are features that allow a user to answer an incoming call that rings on a telephone other than the user's own. For example, if you want everyone in the payroll

department to be able to answer calls to any payroll extension (in case someone is away from their desk), create a pickup group that contains all of the payroll extensions. Members of a pickup group should be located in the same area so that they can hear ringing at the other extensions in the group. Note that extensions can only belong to one pickup group.

- **Call pickup:** Allows users to pick up incoming calls within their own group. The system allows a Location Administrator to select a set of phones to be included in a Pick-up Group. Additional phones can be added to the group, or existing phones within the group can be removed.
- **Group call pickup:** Allows users to pick up incoming calls within their own group or in other groups. Users must dial the appropriate call pickup group number when activating this feature from their phone.

The same procedures apply for configuring both of these features. Group call pickup numbers apply to lines or directory numbers.

Adding a Pickup Group

Procedure

To create a Pickup Group:

- Step 1** Browse to *Location Administration > Pickup Groups*. The *Pickup Group Management* screen is displayed.
- Step 2** Click the **Add** button. The *Add Pickup Group* screen is displayed.
- Step 3** Complete all of the required fields, and then click the **Next** button.
- Step 4** Complete all the required fields on the second screen, and then click the **Add** button.
-

Available pickup group fields include:

Field	Description	Remarks
Name	The name for the Pickup Group.	This is a mandatory field.
Description	A brief description of this Pickup Group.	-
Device Group	The device group to associate with this pickup group.	Select from the drop-down list if required.

Field	Description	Remarks
Pickup Number	<p>The extension number (or free text number) for use by the pickup group.</p> <p>Note</p> <p>The Enter Number radio button (free text field) is only visible if the Customer preference setting <i>AllowFreeTextPickupGroupPilotNumber</i> is either <i>Enabled</i> or <i>Derived from Provider</i> (if configured and enabled).</p>	<p>Select the required radio button, namely <i>Extension</i> or <i>Enter Number</i>. If the <i>Extension</i> radio button is selected, select the required extension from the drop-down list. If the <i>Enter Number</i> radio button is selected, enter the required number in the free text area.</p> <p>Note</p> <p>This number must be unique (not used by any other device).</p> <p>Note</p> <p>When modifying a pickup group, a location administrator (or higher) can change the pickup number from an extension to another extension, from an extension to a free text number, from a free text number to an extension, or from a free text number to another free text number.</p>
Call Pickup Group Notification Policy	The type of notification to users.	Select from the drop-down list.
Call Pickup Group Notification Timer	The seconds of delay (integer in the range of 1 to 300) between the time that the call first comes into the original called party and the time that the notification to the rest of the call pickup group occurs.	Select from the drop-down list.
Calling Party Information	Checkbox to determine if the visual notification message to the call pickup group includes identification of the calling party. The system only makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert.	<p>Disable the checkbox (default) - the feature is off.</p> <p>Enable the checkbox to turn feature on.</p> <p>Note</p> <p>In the case of multiple active notification alerts, the latest visual alert overwrites the previous ones. When a user activates call pickup, the user is connected to the earliest call available for pickup, even if that is not the visual alert currently displayed on the phone. You can avoid this mismatch by using visual notification without displaying calling or called party information.</p>

Field	Description	Remarks
Called Party Information	Checkbox to determine if the visual notification message to the call pickup group includes identification of the called party. The system only makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert.	Disable the checkbox (default) - the feature is off. Enable the checkbox to turn feature on.

Managing a Pickup Group

Procedure

Modifying a Pickup Group

To modify a Pickup Group:

- Step 1** Select the Pickup Group that you wish to modify by selecting the required *Name* (active text link) on the *Pickup Group Management* screen.
- Step 2** Change the required fields and click the **Modify** button. For an explanation of the available fields, see [Adding a Pickup Group on page 906](#).

Note

If the Customer preference setting *AllowFreeTextPickupGroupPilotNumber* is *Disabled*, the Pickup Group Number can only be changed to an extension number.

Procedure

Deleting a Pickup Group

To delete a Pickup Group:

- Step 1** Select the required pickup group *Name* (active text link) on the *Pickup Group Management* screen of the pickup group that you want to manage.
- Step 2** Click the **Delete** button at the bottom-right of the screen.
-

Note

A pickup group cannot be deleted if it still has numbers associated with it. The system requires that you delete all the numbers from the pickup group before deleting it.

See also: [Adding Numbers to a Pickup Group on page 909](#) if you want to add lines/numbers to an existing Pickup Group.

Procedure

Deleting Numbers from a Pickup Group

To remove numbers from an existing pickup group:

- Click the **Delete** button in the *Numbers* section on the *Pickup Group Management* screen, which corresponds with the number you want to delete.

Note

The process deletes the numbers one by one. However, in case you need to delete multiple numbers, you can click the relevant **Delete** button (this should be completed as quickly as possible) without waiting for each of the delete transactions to complete. The system queues the transactions and performs them in turn.

See also: [Associating Pickup Groups on page 910](#) if you want to associate a Pickup Group, where the associated Pickup Groups function as a single Pickup Group.

Procedure***Disassociating Pickup Group***

To disassociate a Pickup Group:

- Step 1** Click the **Disassociate** button in the *Associated Pickup Groups* section on the *Pickup Group Management* screen adjacent to the appropriate Pickup Group.
- Step 2** The Pickup Group is disassociated.

Procedure***Delete a Pickup Group***

To completely delete the Pickup Group, you must disassociate any pickup groups that are associated with it first.

- Step 1** Select the Pickup Group *Name* (active text link) from the *Pickup Group Management* screen that you want to delete.
- Step 2** Click the **Delete** button at the bottom right hand corner on the *Pickup Group Management* screen relevant to the Pickup Group that you want to delete.

Adding Numbers to a Pickup Group**Procedure**

To add numbers to an existing pickup group:

- Step 1** Click the **Add Number** button in the *Numbers* section on the *Pickup Group Management* screen.
- Step 2** Select the required number from the drop-down list and then click the **Add** button. The number is added to the pickup group numbers.

Note

The numbers shown in the drop-down list are the numbers provisioned in the location (both internal extensions and DDIs where applicable).

Procedure***Adding Hunt Group Pilot numbers to a Pickup Group***

To add hunt group pilot numbers to an existing pickup group:

- Step 1** Click the **Add Number** button in the *Numbers* section on the *Pickup Group Management* screen. The *Add Number* screen is displayed.
- Step 2** Select the required extension that corresponds to the Hunt Group pilot number from the drop-down list and then click the **Add** button. The Hunt Group pilot number is added to the system.

Note

The numbers shown in the drop-down list are the numbers provisioned in the location (both internal extensions and DDIs where applicable).

Associating Pickup Groups

When two pickup groups are associated, they function as a single pickup group for as long as they remain associated.

Procedure

To associate a pickup group with another pickup group:

- Step 1** Click the **Associate** button in the *Associated Pickup Groups* section on the *Pickup Group Management* screen.
- Step 2** Select the Pickup Group for association from the drop-down list and then click the **Associate** button. The pickup group is added to the list of associated groups.

Note

The groups shown in the drop-down list are the pickup groups defined in the location which are not yet associated with the current pickup group.

Re-order Pickup Group

When a call in a selected Pickup Group is received the pickup group has an order to determine which Pickup group is called first. The re-order tab is used to change the order of the pickup groups to be answered.

Procedure

- Step 1** Select the Pickup Group *Name* (active text link) you wish to edit from the *Pickup Group Management* screen.
- Step 2** Click the **Re-order** button.
- Step 3** Select the relevant Pickup Group that you wish to move and click the **Move Up/Move Down** buttons as required.
- Step 4** Click the **Update** button when complete to save the changes.

Presence Monitoring

The status of a Presence configuration can be monitored at location level. The monitoring feature displays the following details: the *Extension Number*, the end user's *Username*, an indication of relevant instances (i.e. *All Instances* or *Per Instance*), *Device Name*, *Device Type*, *First Name*, and *Last Name*. The list of DDI numbers associated with an extension is seen by hovering the mouse over the *Extension Number*.

Procedure

To view Presence information at location level:

- Step 1** Browse to *Location Administration > Telephony*.
- Step 2** Select the *Presence Monitoring* active text link.
- Step 3** Enter relevant search criteria and click the **Search** button. A list of extensions that match the entered search criteria is displayed (if any).

Note

No records are displayed until a search is done.

- Step 4** Select the required *Username* (active text link) to modify the Presence configuration for the selected user. Refer to [Managing a Cisco Unified Communications Manager IM and Presence \(IM and Presence\) Server on page 603](#) for detailed information.

Location License Management

Various aspects of location license management are covered, such as available licenses, quotes for license updates and placing orders.

Procedure

Viewing Available Licenses

To view licenses available in the location:

- Step 1** Navigate to *Location Administration > Licenses*.
- Step 2** If required, browse through the relevant hierarchies to the required Location.

The page will display all available licenses for the location:

Field	Description
Services/License Types	The name of the service/license.
Used	The number of service/licenses currently in use.
Remaining	The number of service/licenses remaining to be used.
Reserved	The number of service/licenses reserved for this location.
Description	A description of the service/license.

Procedure

Refreshing the Location License Management page

To refresh the list of available licenses on the *Location License Management* page:

- Step 1** Navigate to *Location Administration > Licenses*.
- Step 2** If required, browse through the relevant hierarchies to the required Location.
- Step 3** Click the **Refresh** button. The list of available licenses will be refreshed.

Procedure***Requesting a Quote for License Updates***

To request a quote for license updates:

Step 1 Navigate to *Location Administration > Licenses*.

Step 2 Click the **Update** button. The following fields are available:

Field	Description
Services/License Types	The name of license.
Used	The number of licenses currently in use.
Remaining	The number of licenses remaining to be used.
Reserved	The number of licenses reserved for this location.
Update Quantity	A number by which to modify the number of reserved licenses.
Action	The action that will be taken when the licenses are updated: <ul style="list-style-type: none"> • Install • Modify • Disconnect
New Amount Reserved	The number of licenses that will be reserved after the update.

Step 3 Modify the relevant fields then request the quote by clicking the **Request Quote** button.

Step 4 After a quote has been requested, the following details are displayed:

Field	Description
Services/License Types	The name of license.
Number of licenses Currently Reserved	The number of licenses currently reserved.
Number of licenses Updates Requested	The number of license updates requested.
Number of licenses Reserved after updates	The number of licenses that will be reserved after the update.
Per unit cost of updates Non Recurring	The per unit non-recurring cost of the updates.
Per unit cost of updates Monthly Recurring	The per unit monthly-recurring cost of the updates.
Total cost of updates Non Recurring	The total non-recurring cost of the updates.
Total cost of updates Monthly Recurring	The total unit monthly-recurring cost of the updates.
Total monthly recur- ring costs Current	The current total monthly-recurring costs.

Field	Description
Total monthly recurring costs	The total monthly-recurring costs after the updates.
After updates	

- Step 5** Click the **Cancel Order** button to cancel the order (optional).

Note

A request for a quote cannot be done when there is any order still pending.

Procedure

Submitting an Order

To place an order after receiving a quote:

- Step 1** Navigate to *Location Administration > Licenses* .
- Step 2** Select the required *quote* (active text link).
- Step 3** Click the **Submit Order** button on the requested quote page. You will be asked to confirm the order before submitting the order.

After the order has been processed, a **status message** is displayed.

Procedure

Viewing ordered Licenses on the Location License Order History page

Follow the steps below to view the list of ordered licenses on the *Location License Order History* page:

- Step 1** Navigate to *General Administration > Order History* or select the **Order History** button on the *View Location Licenses* screen
- Step 2** If required, browse through the relevant hierarchies to the required Location.
- A list of all ordered licenses will be displayed
- To refresh the list, select the **Refresh** button. To view a list of available licenses, select the **Licenses** button.
- Step 3** Select the *Order Id* (active text link) to view a detailed description of any historical order

A summary of the order is displayed and below the summary the order details are displayed, including the following fields:

Field	Description
<i>Order ID</i>	A unique ID of the order.
<i>Date/Time Submitted</i>	The date and time the order was submitted.
<i>Date/Time Completed</i>	The date and time the order was completed.
<i>Submitted by</i>	The user that submitted the order.
<i>Order Status</i>	The current status of the order.

- Step 4** Select the **Refresh** button to update the current view
-

To return to the *View Location Licenses* page, select the **Licenses** button. To return to the *View Order History* page, select the **Order History** button.

Self Care Skinning

The stand-alone *Self Care* section supports skinning. This includes customization of display elements including Cascading Style Sheets, images and page layout.

Themes are managed via theme archives - ZIP files containing styles, images and template files.

A system-wide default theme is provided. This theme can be used as a base for customization. This theme cannot be changed or deleted using the management screens on the system GUI.

Theme Management

The system supports skinning of the web interface via the use of themes. This includes customization of display elements, including Cascading Style Sheets, images and page layout. The themes are managed via a themes archive, a ZIP file containing the styles, images and template files. A system-wide default theme is provided. The default theme can be used as a base for customization but the default theme cannot be changed or deleted using the Theme management screens.

Note

- By default, only system administrators are able to view and manage themes within the system.
 - The ZIP file format (*.ZIP) is a data compression and archive format. A ZIP file contains one or more files that have been compressed to reduce file size, or stored as-is. An application is required to "unzip" (access) a zip file and to create or "zipup" a ZIP file. A number of proprietary and open source compression applications exist such as WinAce®, WinRAR® and WinZip®. A number of mainstream operating systems now include built-in ZIP file support, this functionality is often referred to as *compressed folders*.
-

Procedure

Creating New Themes

To ensure that new themes are compatible with your system, it is recommended that you create new themes by exporting an existing theme and then customizing it.

To create a new theme:

- Step 1** Export an existing theme to your local computer (Follow the Export steps above if needed)
- Step 2** Customize the theme to form the new theme
- Step 3** Once you have finished, re-archive the theme into a ZIP format
-

Important

- The contents of the archive should contain the same directory structure as the exported archive's.

- Themes should be assigned a system-wide, unique, identifying name.

View Themes

Procedure

Follow these steps to view the installed themes:

- Step 1** Browse to *Setup Tools > Self Care Themes*
- A list of all loaded themes will be displayed.
- Step 2** To view details about the files making up a particular theme, select the theme name from the list.

Export Themes

Procedure

Existing themes can be exported and downloaded from the system. This feature can be used as a basis for creating new custom themes, backing up current themes, or deploying themes on a new installation.

Note

When themes are exported, they are saved as ZIP archives.

Follow these steps to export a theme:

- Step 1** Browse to *Setup Tools > Self Care Themes*
- Step 2** A list of all loaded themes will be displayed. Select the **Export** button adjacent to the theme that you would like to export.
- Step 3** Specify where you would like to save the theme and the theme will be saved to the location specified.

Assign Themes

Procedure

Themes can be assigned and unassigned at a provider, reseller or company level.

To assign a theme:

- Step 1** Browse to *Setup Tools > Self Care Themes*
- Step 2** Select the **Assign** button adjacent to the name of a theme in the theme management screen
- Step 3** Select one or more of the providers, resellers and customers from the list and select the **Update** button.

Note

To select multiple entries hold down the *Ctrl* key and make your selection. To select a range of entries, hold down the Shift key and select your start and end entries within the list. To deselect all entries within the list, hold down the *Ctrl* key and select all entries that are still selected.

Assignment is immediate and end users will notice the change the next time they refresh their browser, or browse to a new page within the system. To unassign a theme, follow the steps above but deselect the entities that you want to remove the theme from.

Loading a Theme

Procedure

Adding New Themes

To add a new theme:

- Step 1** Browse to *Setup Tools > Self Care Themes*
 - Step 2** Select the **Add** button
 - Step 3** Provide a name for the theme and then select the **Browse** button
 - Step 4** After selecting the zip file on the local computer, select the **Upload file** button.
-

The new theme will be deployed on the server as soon as the theme archive is uploaded and the contents has been validated.

Modifying and Deleting Themes

Procedure

Modify Existing Themes

Existing themes are modified by exporting the theme archive, modifying the archive contents and uploading the complete theme archive containing all modified theme files.

Follow these steps to modify an existing theme:

- Step 1** Select the **Modify** button next to the required theme name on the theme management screen.
 - Step 2** After having modified the theme on your computer, upload the modified theme to the system.
-

The updated theme will be deployed on the server as soon as the modified theme archive is uploaded and the contents validated.

Note

- Theme names cannot be changed.
 - The default theme cannot be modified.
-

Procedure

Deleting Themes

Existing themes can be deleted from the system.

To delete an existing theme:

- Select the **Delete** button next to the theme name on the theme management screen.

After confirming the deletion, the theme will be deleted from the system.

Note

- The default theme cannot be deleted.
 - A theme cannot be deleted while it is assigned to an entity, please unassign the theme from all entities before deleting it.
-

Migration of themes

If new functionality is added to themes, the existing themes will continue to function as they did in the previous release. However, to make use of the new functionality the recommended migration process is:

Procedure

Migrating themes

- Step 1** Export the default theme. This will include a CSS and an ini file containing all the new theme details.
- Step 2** Adjust the exported files to reflect the required theme (images, colors, text, etc), including all details of the new theme features.
- Step 3** Save the theme, then upload it onto the system to replace the theme which requires the new updated features.

The new theme is now available to any users assigned to that theme.



CHAPTER 9

Appendix

Available Server Fields **919**

ATA Device Parameters **926**

 Basic Device Parameters When Using SIP **926**

 Advanced Device Parameters When Using SIP **926**

Hardware Devices Supported **927**

 Phone Types **927**

 Expansion Modules **931**

 Miscellaneous Devices **931**

 IOS Gateway Hardware **932**

Available Preferences and Settings **934**

 Using System Preferences **934**

 Location Preference and Settings **935**

 Provider Preference and Settings **937**

 Division Preference and Settings **942**

 Customer Preference and Settings **942**

 Reseller Preferences and Settings **946**

 System Preference and Settings **946**

 Building Preferences **949**

 Dial Plan Preference and Settings **950**

Operations Tools **950**

Upgrade Limitations **966**

Unified CM Group Allocation Logic **967**

 Overview **967**

 Adding a New CCM Group to the Cluster **967**

 Caveats and Limitations **968**

Available Server Fields

Note

Depending on the configuration of your system, available fields may differ.

CCM Server

Field	Description
Software Version	This is a mandatory field. Select the software version that the server will be running. For example, CCM: 4.1.3 or CCM: 4.2.0.
Name	This is a mandatory field. The name of the server. This server name must be unique in the system.
Description	A short description of the server.
Publisher Host Name	<p>This is a mandatory field. Hostname for the server where the Unified Communications Manager is installed. The actual hostname of the server must be used.</p> <p>Note</p> <p>If Cisco Unified Communications Manager (Unified CM) 5 or later is being used, an IP Address may NOT be used for this value. To identify the host name of the server in version 5 onwards, use the Unified CM CLI command <code>show network cluster</code>.</p>
Publisher CCM Name	This is a mandatory field. CCM name for the server where the Unified CM is installed. This is the name of the server as shown in Unified CM (typically the IP Address of the server). This value can be found by browsing to <i>System -> Cisco Unified CM</i> .
Publisher IP Address	This is the IP address used by CUCDM when communicating with the Unified CM server. This is only true for the publisher. This is also the address that is used to create trunks (publisher and subscribers) between PBXs. This is a mandatory field.
Publisher IP Address B	This IP address is available for use by Gateways when communicating with the Unified CM server. A Gateway option allows the user to specify whether the normal IP Address or this address is used. This allows support for various NAT configurations. See the IOS Gateways Guide for details on how to use these settings/options.
Publisher Config User name	This is a mandatory field. The user name for configuring the server.
Publisher Config Password	<p>This is a mandatory field. The password to be used when configuring the server.</p> <p>Note</p> <p>Due to a known issue with the Unified CM password algorithm, please ensure that you do not include the "@" symbol in the password.</p>

Field	Description
Domain Name	<p>The value entered in this field will be used to apply a new domain name to all registered Cisco Dual Mode for Android devices.</p> <p>Note</p> <ul style="list-style-type: none"> To apply the domain name to devices, the Operations Tool Apply Domain Name to Android devices must be run. The field is limited to 50 alphanumeric characters in length, including these punctuation symbols: space, period, hyphen and underscore.
Country	This is a mandatory field. Select the country within which the server will be situated from the drop-down list.
Annunciator Server	Select this checkbox if the server is going to be used as an Annunciator server.
EMCC Server	Select this checkbox if the server is going to be used as an EMCC server. Select the required server order from the drop-down list if required.
Annunciator Line Capacity	If you have selected the Annunciator Server checkbox, use this field to specify the number of Annunciator Lines that will be available.
Conference server	Select this checkbox if the server is going to be used as a Conference server.
Conference Streams	If you have selected the conference server checkbox, use this field to specify the number of conference streams/lines that will be available.
IP PBX	This is a mandatory field. Select this checkbox if the server is going to be used as an IP PBX.
IPPBX lines	If you have selected the IP PBX checkbox, use this field to specify the number of IPPBX Lines that will be available.
Max. IPPBX lines per device	If you have selected the IP PBX checkbox, use this field to specify the maximum number of IPPBX Lines that will be available for use by each device.
Media Termination Point	Select this checkbox if the server is going to be used as a Media Termination Point.
Media Termination Point Line Capacity	If you have selected the Media Termination Point checkbox, use this field to specify the line capacity of the Media Termination Point.
Music server	Select this checkbox if the server is going to be used as a Music Server. Select the required server order from the drop-down list if required.
Music lines	If you have selected the Music server checkbox, use this field to specify the number of Music Lines that will be available.
Switchboard/Console server	Select this checkbox if the server is going to be used as a Switchboard/Console server.
Console lines	If you have selected the Switchboard/Console server checkbox, use this field to specify the number of Console lines that will be available.

Field	Description
TFTP server	Select this checkbox if the server is going to be used as a TFTP server. Select the required server order from the drop-down list if required.
CPID	This is a mandatory field. If you would like the system to automatically select the required value, select the <i>Auto</i> option, alternatively, select the required value from the drop-down list.
ClusterID	This is a mandatory field. If you would like the system to automatically select the required value, select the <i>Auto</i> option, alternatively, select the required value from the drop-down list.
Manual configuration Mode?	<p>Select this checkbox if you would like the server to operate in manual configuration mode. This option should be used for un-managed clusters.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>
Email address for Manual activation	<p>The email address that will be used for manual activation of the CCM Server.</p> <p>Note</p> <p>It is mandatory to provide an email address if the Manual configuration Mode option is selected.</p>
Network Monitoring active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note</p> <p>Depending on network loads, selecting this option may impact on the performance of the server.</p>
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	<p>Select this option if you would like all configuration sessions with the server to be encrypted.</p> <p>Note</p> <p>While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.</p>

IP Unity Server

Field	Description
Details	
Host Name	This is a mandatory field. Host name for the server. Must be unique in the system.
IP Address	This is a mandatory field. IP Address for the server.
Description	A short description of the server.
Config User Name	This is a mandatory field. The user name for configuring the server.
Config Password	This is a mandatory field. The password to be used when configuring the server.
Software Version	This is a mandatory field. Select the software version that the server will be running, alternatively, you can select the <i>Any</i> option.
Maximum Lines supported	This is a mandatory field. The maximum number of lines that the server will support.
CPID	This is a mandatory field. If you would like the system to automatically select the required value, select the <i>Any</i> option, alternatively, select the required value from the drop-down list.
Manual configuration Mode?	<p>Select this checkbox if you would like the server to operate in manual configuration mode. This option should be selected for un-managed clusters.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>
Email address for Manual activation	The email address that will be used for manual activation of the IP Unity Server.
Network Monitoring active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note</p> <p>Depending on network loads, selecting this option may impact on the performance of the server.</p>
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Roles	
Conference server	Select this checkbox if the server is going to be used as a Conference server.
IVR server	Select this checkbox if the server is going to be used as an IVR server.
Voicemail server	Select this checkbox if the server is going to be used as a Voice-mail server.

PGW

Field	Description
PGW Details	
Name	<p>This is a mandatory field. This is the name of the PGW, where a PGW may be a single server or dual server deployment.</p> <p>It should be noted that the '&' character must not be used in this field in version 3.0.8</p>
Description	A short description of the PGW
Software Version	This is a mandatory field. This defines the software version running. This must be set correctly to ensure correct operation.
Manual configuration Mode?	<p>Select the checkbox if the system is not going to be used to configure this device.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>
Email address for Manual activation	If the Manual configuration Mode box is checked, an email address must be entered. This email address should be for the person or group that will perform the manual configuration of the device.
Network Monitoring Active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note</p> <p>Depending on network loads, selecting this option may impact on the performance of the server.</p>
Line Capacity	Defines the number of PSTN Lines/Channel available via this PGW.
Country	Defines the country that the PGW is located in.
Call Processor Id	This Id is used for internal call routing and may either be selected by the administrator or if AUTO is selected, the system will automatically allocate the Id.
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	<p>Select this option if you would like all configuration sessions with the server to be encrypted.</p> <p>Note</p> <p>While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.</p>
Main PGW Server Details	
Note: The following are repeated if a Backup PGW server is used.	
Host Name	This is a mandatory field. This is the DNS host name of the server.

Field	Description
Primary IP Address	A PGW may have either one or two network interfaces with an IP Address. This is the Primary IP Address and is the interface that the system will initially use to connect to the PGW.
Secondary IP Address	This is the Secondary IP Address and is the interface that the system will use if a connection is not possible via the primary interface.
Config User ID (Name)	The PGW server login user name required to configure the PGW.
Config Password	The PGW login password, required to configure the PGW.
Config Prompt	The PGW server prompt displayed when logged using the Config user name. This value is only used if telnet is used to configure the PGW.
MML Command	The system configures the PGW using PGW mml commands. This attribute defines the command used to start an mml session. The default value is mml -s12.
FTP Path	Defines the location on the PGW server to which the system transfers the PGW config files.

Technician Server

Field	Description
Host Name	This is a mandatory field. The Host name for the technician server, which must be unique in the system.
IP Address	This is a mandatory field. The IP address of the server being added. The IP address must be unique within the system.
Email Address	This is a mandatory field. The email address of the person responsible for the server.
Description	An optional description of the server.
Role	This field cannot be modified and will be auto-populated by the system.
Lines	Depending on the role specified above, you may be asked to specify aspects such as the number of lines available.

Cisco 36xx Server

Field	Description
Host Name	This is a mandatory field. Must be unique in the system.
IP Address	This is a mandatory field. The IP address of the server being added. The IP address must be unique within the system.
Description	A short description of the server.
Cisco User Id Required?	Select this checkbox if you would like to force users to use a Cisco User ID to access the server.
Config User name	This is a mandatory field. The user name for configuring the server.
Config Password	This is a mandatory field. The password to be used when configuring the server.
Enable Password	Select this checkbox to force the use of the password.
Version	Select the version of server from the drop-down list.

Field	Description
Manual configuration Mode?	<p>Select this checkbox if you would like the server to operate in manual configuration mode. This option should be used for un-managed clusters.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>
Email address for Manual activation	The email address that will be used for manual activation of the CCM Server.
Network Monitoring active?	<p>Select this checkbox if you would like the server to activate Network Monitoring.</p> <p>Note</p> <p>Depending on network loads, selecting this option may impact on the performance of the server.</p>
Detailed trace file of configuration sessions?	Select this checkbox to enable the server to maintain a detailed log file of all configuration sessions.
Encrypt configuration sessions?	<p>Select this option if you would like all configuration sessions with the server to be encrypted.</p> <p>Note</p> <p>While the use of encryption is recommended, diminished performance may be experienced depending on the performance of your network.</p>

ISC Server

Field	Description
Host Name	This is a mandatory field. Must be unique in the system.
Description	A short description of the server.
IP Address	This is a mandatory field. The IP address of the server being added. The IP address must be unique within the system.
Config User name	The user name for configuring the server.
Config Password	The password to be used when configuring the server.
Path and name of config file	The location and name of the configuration file to be used.
Path and name of leases file	The location and name of the IP lease file to be used.
Version	The ISC version to be used.
Manual Configuration Mode?	<p>Select this checkbox if you would like the server to operate in manual configuration mode. This option should be selected for un-managed clusters.</p> <p>Note</p> <p>It is mandatory to provide an email address if this option is selected.</p>
Email address for Manual activation	The email address that will be used for manual activation of the CCM Server.

Field	Description
Network Monitoring active?	Select this checkbox if you would like the server to activate Network Monitoring. Note Depending on network loads, selecting this option may impact on the performance of the server.

ATA Device Parameters

Basic Device Parameters When Using SIP

Parameter	Value
Name	Third-party SIP Device (Basic)
Description	Third-party SIP Device (Basic)
Product	Third-party SIP Device (Basic)
Product Model ID	336
Protocol	SIP
Hostname Prefix	SEP
Max Number of Lines	1
Max number of speed dials	0
Max. Number of Busy Lamp Fields	0
Max. Number of Softkeys	0
Max. Number of Buttons	0
Screen available	No
Color Screen	No
Max. Calls Waiting	2
Default Max. Number of Calls Waiting	2
Max. Busy Trigger Value	2
Default Max. Busy Trigger Value	2
Max. No Answer Ring Duration (secs)	180
Default Max. No Answer Ring Duration (secs)	12
Expansion Module Capable (check for Yes)	No

Advanced Device Parameters When Using SIP

Parameter	Value
Name	Third-party SIP Device (Advanced)
Description	Third-party SIP Device (Advanced)
Product	Third-party SIP Device (Advanced)
Product Model ID	374
Protocol	SIP
Hostname Prefix	SEP
Max Number of Lines	2
Max number of speed dials	0

Parameter	Value
Max. Number of Busy Lamp Fields	0
Max. Number of Softkeys	0
Max. Number of Buttons	0
Screen available	No
Color Screen	No
Max. Calls Waiting	16
Default Max. Number of Calls Waiting	2
Max. Busy Trigger Value	16
Default Max. Busy Trigger Value	2
Max. No Answer Ring Duration (secs)	180
Default Max. No Answer Ring Duration (secs)	12
Expansion Module Capable (check for Yes)	No

Hardware Devices Supported

The system supports the following device types, which are listed under Phone Types, Expansion Modules, Miscellaneous Devices, and IOS Gateway Hardware below:

Phone Types

The following phone types/handsets are added by the default *Base Bulk loader sheet* :

Name	Product Name / Description
7960	Cisco 7960
Cisco 3905 SIP	Cisco 3905 SIP
Cisco 3911 SIP	Cisco 3911 SIP
Cisco 3951 SIP	Cisco 3951 SIP
Cisco 6901	Cisco 6901
Cisco 6901 SIP	Cisco 6901 SIP
Cisco 6911	Cisco 6911
Cisco 6911 SIP	Cisco 6911 SIP
Cisco 6921	Cisco 6921
Cisco 6921 SIP	Cisco 6921 SIP
Cisco 6941	Cisco 6941
Cisco 6941 SIP	Cisco 6941 SIP
Cisco 6945	Cisco 6945 SCCP
Cisco 6945 SIP	Cisco 6945 SIP
Cisco 6961	Cisco 6961
Cisco 6961 SIP	Cisco 6961 SIP
Cisco 7821	Cisco 7821 SIP
Cisco 7841	Cisco 7841 SIP
Cisco 7861	Cisco 7861 SIP
Cisco 7902	Cisco 7902
Cisco 7905	Cisco 7905

Name	Product Name / Description
Cisco 7905 SIP	Cisco 7905 SIP
Cisco 7906	Cisco 7906
Cisco 7906 SIP	Cisco 7906 SIP
Cisco 7910	Cisco 7910
Cisco 7911	Cisco 7911
Cisco 7911 SIP	Cisco 7911 SIP
Cisco 7912	Cisco 7912
Cisco 7912 SIP	Cisco 7912 SIP
Cisco 7920	Cisco 7920
Cisco 7921	Cisco 7921
Cisco 7925	Cisco 7925
Cisco 7926	Cisco 7926
Cisco 7931	Cisco 7931
Cisco 7931 SIP	Cisco 7931 SIP
Cisco 7935	Cisco 7935
Cisco 7936	Cisco 7936
Cisco 7937	Cisco 7937
Cisco 7940	Cisco 7940
Cisco 7940 SIP	Cisco 7940 SIP
Cisco 7941	Cisco 7941
Cisco 7941 SIP	Cisco 7941 SIP
Cisco 7941G-GE	Cisco 7941G-GE
Cisco 7941G-GE SIP	Cisco 7941G-GE SIP
Cisco 7942	Cisco 7942
Cisco 7942 SIP	Cisco 7942 SIP
Cisco 7945	Cisco 7945
Cisco 7945 SIP	Cisco 7945 SIP
Cisco 7960	Cisco 7960
Cisco 7960 SIP	Cisco 7960 SIP
Cisco 7961	Cisco 7961
Cisco 7961 SIP	Cisco 7961 SIP
Cisco 7961G-GE	Cisco 7961G-GE
Cisco 7961G-GE SIP	Cisco 7961G-GE SIP
Cisco 7962	Cisco 7962
Cisco 7962 SIP	Cisco 7962 SIP
Cisco 7965	Cisco 7965
Cisco 7965 SIP	Cisco 7965 SIP
Cisco 7970	Cisco 7970
Cisco 7970 SIP	Cisco 7970 SIP
Cisco 7971	Cisco 7971
Cisco 7971 SIP	Cisco 7971 SIP

Name	Product Name / Description
Cisco 7975	Cisco 7975
Cisco 7975 SIP	Cisco 7975 SIP
Cisco 7985	Cisco 7985
Cisco 8831 SIP	Cisco 8831 SIP
Cisco 8841	Cisco 8841
Cisco 8851	Cisco 8851
Cisco 8861	Cisco 8861
Cisco 8941 SIP	Cisco 8941 SIP
Cisco 8941	Cisco 8941 SCCP
Cisco 8945 SIP	Cisco 8945 SIP
Cisco 8945	Cisco 8945 SCCP
Cisco 8961 SIP	Cisco 8961 SIP
Cisco 9945 SIP	Cisco 9945 SIP
Cisco 9951 SIP	Cisco 9951 SIP
Cisco 9965 SIP	Cisco 9965 SIP
Cisco 9971 SIP	Cisco 9971 SIP
Cisco ATA 186	Cisco ATA 186
Cisco ATA 186 SIP	Cisco ATA 186 SIP
Cisco ATA 187 SIP	Cisco ATA 187 SIP
Cisco Cius	Cisco Cius
Cisco Cius SP	Cisco Cius SP
Cisco Dual Mode for Android	Cisco Dual Mode for Android
Cisco E20	Cisco E20
Cisco IP Communicator	Cisco IP Communicator
Cisco IP Communicator SIP	Cisco IP Communicator SIP
Cisco Jabber Client	Cisco Jabber Client
Cisco Jabber for Tablet	Cisco Jabber for Tablet
Cisco Jabber IM	Cisco Jabber IM
CUCI-CSF	Cisco Unified Client Services Framework
CUCICONNECT	Cisco Unified Client Integration for Webex Connect
CUCIMOC	Cisco Unified Client Integration for Microsoft Office Communicator
CUPC-CSF	Cisco Unified Client Integration for Cisco Unified Personal Communicator
CUPC SIP	Cisco Unified Personal Communicator SIP
iPhone	Cisco Dual Mode for iPhone
Nokia S60	Nokia S60
Nokia SCCP	Nokia SCCP
Third-party SIP Device (Advanced)	Third-party SIP Device (Advanced)
Third-party SIP Device (Basic)	Third-party SIP Device (Basic)
Cisco TelePresence EX60	Cisco TelePresence EX60

Name	Product Name / Description
Cisco TelePresence EX90	Cisco TelePresence EX90
Cisco TelePresence SX10	Cisco TelePresence SX10
Cisco TelePresence SX20	Cisco TelePresence SX20 (CUCM 9.x)
Cisco TelePresence SX80	Cisco TelePresence SX80
Cisco TelePresence MX200	Cisco TelePresence MX200 (CUCM 9.x)
Cisco TelePresence MX200 G2	Cisco TelePresence MX200 G2
Cisco TelePresence MX300	Cisco TelePresence MX300 (CUCM 9.x)
Cisco TelePresence MX300 G2	Cisco TelePresence MX300 G2 (CUCM 9.x)
Cisco TelePresence TX9000	Cisco TelePresence TX9000 (CUCM 9.x)
Cisco TelePresence TX9200	Cisco TelePresence TX9200 (CUCM 9.x)
Cisco TelePresence	Cisco TelePresence
Cisco TelePresence 1000	Cisco TelePresence 1000
Cisco TelePresence 1100	Cisco TelePresence 1100
Cisco TelePresence 1300-47	Cisco TelePresence 1300-47
Cisco TelePresence 1300-65	Cisco TelePresence 1300-65
Cisco TelePresence 1310-65	Cisco TelePresence 1310-65
Cisco TelePresence 3000	Cisco TelePresence 3000
Cisco TelePresence 3200	Cisco TelePresence 3200
Cisco TelePresence 500-32	Cisco TelePresence 500-32
Cisco TelePresence 500-37	Cisco TelePresence 500-37
Cisco TelePresence Codec C40	Cisco TelePresence Codec C40
Cisco TelePresence Codec C60	Cisco TelePresence Codec C60
Cisco TelePresence Codec C90	Cisco TelePresence Codec C90
Cisco TelePresence Quick Set C20	Cisco TelePresence Quick Set C20
Cisco Telepresence Profile 42 (C20)	Cisco Telepresence Profile 42 (C20) 9.x
Cisco TelePresence Profile 42 (C40)	Cisco TelePresence Profile 42 (C40) 9.x
Cisco Telepresence Profile 42 (C60)	Cisco Telepresence Profile 42 (C60) 9.x
Cisco Telepresence Profile 52 (C40)	Cisco Telepresence Profile 52 (C40) 9.x
Cisco Telepresence Profile 52 (C60)	Cisco Telepresence Profile 52 (C60) 9.x
Cisco Telepresence Profile 52 Dual (C60)	Cisco Telepresence Profile 52 Dual (C60) 9.x
Cisco Telepresence Profile 65 (C60)	Cisco Telepresence Profile 65 (C60) 9.x
Cisco Telepresence Profile 65 Dual (C90)	Cisco Telepresence Profile 65 Dual (C90) 9.x
Cisco 12 S	Cisco 12 S
Cisco 12 SP	Cisco 12 SP
Cisco 12 SP+	Cisco 12 SP+
Cisco 30 SP+	Cisco 30 SP+
Cisco 30 VIP	Cisco 30 VIP
Generic Desktop Video Endpoint	Generic Desktop Video Endpoint
Generic Multiple Screen Room System	Generic Multiple Screen Room System
Generic Single Screen Room System	Generic Single Screen Room System
IP-STE	IP-STE

Name	Product Name / Description
Transnova S3	Transnova S3
IMS-integrated Mobile (Basic)	IMS-integrated Mobile (Basic)
Cisco Virtualization Experience Client (VXC 6215)	Cisco Virtualization Experience Client (VXC 6215) (CUCM 9.x)
Third-party AS-SIP Endpoint	Third-party AS-SIP Endpoint(CUCM 9.x)
Cisco Jabber for Tablet	Cisco Jabber for Tablet (CUCM9.x)
Carrier-integrated Mobile	Carrier-integrated Mobile (CUCM 9.x)
CTI Remote Device	CTI Remote Device (CUCM 9.x)
Cisco DX650	Cisco DX650 SIP

Expansion Modules

The following Expansion Module types are added by the default *Base Bulk loader sheet* :

Name	Number of Buttons / Lines	Protocol
7914	14	SCCP
7915-12	12	SCCP
7915-12 SIP	12	SIP
7915-24	24	SCCP
7915-24 SIP	24	SIP
7916-12	12	SCCP
7916-12 SIP	12	SIP
7916-24	24	SCCP
7916-24 SIP	24	SIP
IP Color Expansion Module-36	36	SIP

Miscellaneous Devices

The following miscellaneous devices are added by the default *Base Bulk loader sheet*:

Device	Brief Description
Technician	A General purpose product
PGW	Cisco Transit switch
HSI	H.323 Signaling Interface for PGW
CUCM	Cisco Unified Communications Manager
ISC	ISC.org DHCP server
Cisco36xx	Cisco 36xx series Router
IPUnity	IPUnity Voice Mail Server
IOSDevice	Generic Cisco IOS Device
CiscoSRST	Cisco SRST capable Router
CiscoEmergencyResponder	Cisco Emergency Responder
PGW_TimesTen	Cisco Transit Switch Database
UnmanagedPBX	Unmanaged PBX
Unity	Cisco Unity Voice Mail Server
Netwise	Switchboard/Console server

Device	Brief Description
UnityConnection	Cisco Unity Connection Voice Mail Server
SME	Cisco Session Manager
UnifiedPresence	Cisco Unified Presence Server
UC Central	UC Central Unified Communicator
WebEx	Cisco WebEx Conference Server
UCCE	Unified Contact Center Enterprise

IOS Gateway Hardware

CUCDM supports the following IOS gateway hardware, which includes chassis, ports as well as network modules:

Item
AIM-VOICE-30
Analog Phone
C881VA-V
C887VA-V
Cisco 1751
Cisco 1760
Cisco 1861
Cisco 269X
Cisco 26XX
Cisco 2801
Cisco 2811
Cisco 2821
Cisco 2851
Cisco 2901
Cisco 2911
Cisco 2921
Cisco 2951
Cisco 362X
Cisco 364X
Cisco 366X
Cisco 3725
Cisco 3745
Cisco 3825
Cisco 3845
Cisco 3925
Cisco 3925E
Cisco 3945
Cisco 3945E
Cisco 881
Cisco 888/887/886

Item
Cisco Catalyst 4000 Access Gateway Module
Cisco Catalyst 4224 Voice Gateway Switch
Cisco Catalyst 6000 12 port FXO Gateway
Cisco Catalyst 6000 24 port FXS Gateway
Cisco Catalyst 6000 E1 VoIP Gateway
Cisco Catalyst 6000 T1 VoIP Gateway
Cisco IAD2400
Cisco MGCP BRI Por
Cisco MGCP E1 Por
Cisco MGCP FXO Por
Cisco MGCP FXS Por
Cisco MGCP T1 Por
Cisco VG200
Cisco VG248 Gateway
Cisco VGC Virtual Phone
Cisco VGD-1T3
Communication Media Module
FLEX_SLO
IAD2400_ANALOG
IAD2400_DIGITAL
ISDN BRI Phone
NM-1V
NM-2V
NM-4VWIC-MBRD
NM-HD-1V
NM-HD-2V
NM-HD-2VE
NM-HDA
NM-HDV
NM-HDV2-0POR
NM-HDV2-1POR
NM-HDV2-2POR
PA-MCX
PA-VXA
PA-VXB
PA-VXC
PRODUCT_CAT_4000_ACCESS_GATEWAY_MODULE
VG202
VG204
VG224
VG350

Item
VGC Por
VIC_SLO
VNM-HDA
VWIC_SLO
WS-SVC-CMM-MS
WS-X6600

Available Preferences and Settings

Global Settings are a collection of high level system preferences that enable administrators to perform system wide changes to the system.

Note

Preferences within Global settings can have far reaching impacts within the system, always ensure you understand the full consequences before running one of these preferences.

Available preferences may differ depending on the configuration of your system.

Preferences can be accessed from a number of different locations, such as the *Global Settings > Preferences and Settings : System* page and the *General Administration > Locations > Location Management* page.

Depending on your user level, the range of available preferences differ. For information on the available preferences, select the relevant link (active text link) below:

- [Location Preference and Settings on page 935](#)
- [Provider Preference and Settings on page 937](#)
- [Division Preference and Settings on page 942](#)
- [Customer Preference and Settings on page 942](#)
- [Reseller Preferences and Settings on page 946](#)
- [Building Preferences on page 949](#)
- [System Preference and Settings on page 946](#)
- [Dial Plan Preference and Settings on page 950](#)

For instructions on how to use these preferences, refer to [Using System Preferences on page 934](#).

Using System Preferences

Global Settings are a collection of high level system preferences that enable administrators to perform system wide changes to the system.

Note

- Preferences within the Global Settings page can have far reaching impacts within the system, always ensure you understand the full consequences before running one of these preferences.
- Available preferences may differ depending on the configuration of your system, view a list of the available preferences is here: [Available Preferences and Settings on page 934](#).

- System Preferences can be accessed from a number of locations, including the *Global Settings* menu and the *Location Management* page.

Procedure

Running a System Preference

To use one of the system preferences:

- Step 1** Navigate to *Setup Tools > Global Settings*. The *Preferences and Settings : System* screen is displayed.
- Step 2** Select the system preference *Name* (active text link) that you would like to run.
- Step 3** Specify any required variable and/or options, and then click the **Modify** button. The system preference run and the relevant changes are made to the system.

Location Preference and Settings

Tool	Description	Impact and Limitations of Tool
AssociateFNNinRanges	Associate FNN in PGW in ranges.	In case the preference is set on, the Association and Disassociation of FNNs in the PGW is set in ranges. The ranges available are of 1, 10, 100, 1000 numbers. This allows for a much faster association/dis-association process, however, once the preference is set on and any association is done, the system does not allow you to turn it off until all ranges of FNNs in this location have been disassociated.
AutoDevicePoolLocation	Location device pool to use during auto registration.	Select the required device pool from the drop-down list. The selected device pool is assigned to devices that have been auto registered to this location. If this preference has never been set, the location's default device pool is used.
AutoFeatureLocation	Feature Group for Phone based registration for this location.	Relevant only in conjunction with AutoRegister and AutoRegister-LowestLocation. If the AutoFeatureCustomer preference is not enabled, enabling the AutoFeatureLocation preference has no impact on the system. However, disabling the AutoFeatureLocation preference while the AutoFeatureCustomer preference is enabled disables the AutoFeature functionality for the selected location.
AutoLastResortFeatureLocation	Feature Group for Last Resort Phones at this location.	-

Tool	Description	Impact and Limitations of Tool
AutoMoveLocation	Allow Auto Move of Phone to this location.	If enabled, the system identifies a new phone connected to the location edge device (switch) and uses this information to move the phone into the location providing it with an IP address from the location subnet without the need for manual intervention by the administrator. This is done only for phones that are unassigned. If the AutoMoveCustomer preference is not enabled, enabling the AutoMoveLocation preference has no impact on the system. However, disabling the AutoMoveLocation preference while the AutoMoveCustomer preference is enabled disables AutoMove for the selected location.
AutoRegister	Automate the registration of phones at a location.	Automatic Registration of the phone after it has been moved to the location. Works in conjunction with AutoFeatureLocation and AutoRegisterLowestLocation
AutoRegisterLowestLocation	Lowest allowed extension number for automatic registration at this location.	Phones automatically registered use numbers consecutively starting from this value. This is relevant only in conjunction with AutoFeatureLocation and AutoRegister If the AutoRegisterLowestCustomer preference is not enabled, enabling the AutoRegisterLowestLocation preference has no impact on the system. However, disabling the AutoRegisterLowestLocation preference while the AutoRegisterLowestCustomer preference is enabled disables the AutoRegisterLowest functionality for the selected location.
LocationDefaultLoginPassword	Use the default password to reset user passwords	In case there is a set value in this preference, this becomes the default password assigned to any user requiring reset of their password. If this contains a value, it overrides the default login preference from any parent entity. Default - no value.

Tool	Description	Impact and Limitations of Tool
LocationDefaultVoicemailPassword	Use the default password to reset voicemail passwords.	In case there is a set value in this preference, this becomes the default Voicemail box password assigned to any user requiring reset of their Voicemail box password. If this contains a value, it overrides the default login preference from any parent entity. Default - no value.
LocationLocalCLIR	Location has Calling Line Id Restricted for local calls	-
LocationPhoneDisplay-1st-line	Text to insert on first line of Phone display.	Only include the digits 0 to 9, *, #, X and +. Maximum length = 24. Default - no value.
PersonalisePhoneApplications	Allow personalization of phone application.	This functionality is not available via feature groups or user mobility profiles.
ShowTenantDirectory	Display Tenant Directory on phones.	-
XML-LoginDuration	Time in seconds to expire Users login.	Best Practice: If users always use their mobility profile and are not expected to log out of their phones, set this value as high as possible (e.g. 50,000,000)
XML-PhoneBasedPinReset	Selecting this option enables users to change their PIN via phone services on their phone.	
XML-PhoneBasedUnregister	Allow Installer to Unregister phone from the Services menu.	-

Provider Preference and Settings

Tool	Description	Impact and Limitations of Tool
AllowDuplicateIpAddresses	Used to determine the extent to which an IOS Gateway can share its IP address.	If enabled (checkbox selected), an IOS Gateway can share its IP Address with another IOS Device (as long as the other IOS Device is within a different Customer).

Tool	Description	Impact and Limitations of Tool
BVSMUserRoaming	Use login during User Extension Mobility function.	<p>When this setting is enabled (checkbox selected), the roaming login/logout service in the system (CUCDM) is used. If the setting is disabled, the login/logout service on the Cisco Unified Communications Manager (Unified CM) is used.</p> <p>Note</p> <p>If the setting is disabled while extension mobility location groups exist for the provider, all extension mobility location groups for the provider will be deleted.</p>
DeviceGroupsSupported	Enable the use of device groups.	-
FeatureGroupEditRestrictedToReseller	The end users feature group setting is unmodifiable on the manage end user screen for all customer administrators and below.	Only the provider administrator has access to edit this setting.
FreeTextPickupGroupPilotNumber	Free Text Pickup Group Pilot Number.	<p>Enable (select) or Disable as required.</p> <p>The value of this setting is used by customers that have the <i>AllowFreeTextPickupGroupPilotNumber</i> set to <i>Derived from Provider</i> to determine whether to display or hide the free text pilot number feature.</p>

Tool	Description	Impact and Limitations of Tool
FreeTextPickupGroupPilotNumber-AdminRoles	Free Text Pickup Group Pilot Number Admin Roles.	<p>Used to determine which logged in administrator can access the Pick-up Groups free text pilot number feature (if it is enabled at that customer). Select the required option from the drop-down list:</p> <ul style="list-style-type: none"> • Provider Admin (and above) • Reseller Admin (and above) • Customer Admin (and above) • Division Admin (and above) • Location Admin (and above) <p>These options are hierarchical, so if the setting is set to <i>Location Admin (and above)</i>, then location administrators and above (all administrators since they are all above location admin) can access the new feature. Setting a role preference gives access to all administrators in that role.</p>
LocalGWVoicemailCallRoutingSupport	LocalGW Voicemail Call Routing Support. This preference is used to control the provisioning of an additional LocationVM model for Local GW support (see Note 1 below this table).	If this preference is set to true, the additional model applies to any configuration specifically required for local gateway support with voicemail.
MoviusAAHotlinkLogin		This setting does not apply to Cisco HCS.
MoviusSSO		This setting does not apply to Cisco HCS.
MultiTenantVoicemail	Multi Tenant Voicemail.	<p>If MultiTenantVoicemail is enabled (checkbox selected), then Voicemail Service is at Customer level. If MultiTenantVoicemail is disabled (checkbox not selected), then Voicemail Service is at Provider level.</p> <p>A voicemail service cannot be added for a HCS dial plan when MultiTenantVoicemail is disabled. When MultiTenantVoicemail is enabled for a HCS dial plan, the MultiTenantVoicemail setting cannot be updated to 'disabled'.</p>

Tool	Description	Impact and Limitations of Tool
ProviderAllowAutoPhoneInventory	Allow phones to be automatically added to inventory if detected.	-
ProviderDefaultLoginPassword	Use the default password to reset user passwords.	-
ProviderDefaultVoicemailPassword	Use the default password to reset voicemail passwords.	-
SharedWANBandwidth	Allow WAN Bandwidth to be shared between Customers and Locations. The default for this setting is False.	If this is set to true, the Cisco Unified Communications Manager (Unified CM) location creation behavior is different. This enables multiple locations to share a single Unified CM location for bandwidth (Call Admission Control) purposes (see Note 3 below this table).

Tool	Description	Impact and Limitations of Tool
UsernameValidation	Allow for the validation of the username to be enabled or disabled. The default for this setting is that validation is enabled.	<p>If this setting is enabled, the characters in a username of Admin and End users are validated within the following range: A-Z a-z 0-9 _ @ -</p> <p>Note</p> <p>The @ character is not supported by a mobility profile in the Unified CM. Additional characters not supported by a mobility profile in the Unified CM include special characters such as / \ [] { } () " ' and :</p> <p>If the setting is disabled, the characters in a username are not validated. However, refer to the note below.</p> <p>Note</p> <ul style="list-style-type: none"> The system uses the username as a mobility profile name in Unified CM. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores. Note that the backslash \ is not a valid character. When user name validation is off, it is not recommended to add users with a right round bracket, i.e.) in the user name. Currently this allows voicemail to be added for this user, but will disallow any further modification or deletion of the voicemail account.

Note 1: For LocalGWVoicemailCallRoutingSupport:

- If this is enabled for the provider, then during the AddLocationVM transaction, an additional Cisco Unified Communications Manager (Unified CM) model call is made using the model name AddLocationVMLocalGW-<networkdevicetype> (e.g. AddLocationVMLocalGW-IPUnity). This model can be used to apply any config specifically required for LocalGW support with voicemail.
- This model is not called during the DelLocationVM transaction, so any configuration applied remains on the Unified CM after deletion.
- This model currently supports the Route Patterns sheet in the loader and the variable #VMCPID# which is the CPID of the voicemail server used by the voicemail service assigned to the location.

- This model is never called for a delete, so the Route Patterns would be left behind after locations are deleted.

Note 3: For Shared Bandwidth:

- If the SharedWANBandwidth setting is false, Unified CM location is per location in the system, using the format of Location setting from global settings and \$location_id (e.g. location-bvsm-23). If the setting is true, a Unified CM location is created for the edge device using the format of location setting from global settings and the IP edge device name (e.g. location-bvsm-IPEdge1). A system location uses the Unified CM location of the IP edge device - so all phones are in location-bvsm-IPEdge1.
- Once a location has been deployed within the Provider, the SharedWANBandwidth setting cannot be updated. Shared Bandwidth can however be managed at a location level using the IP Edge Devices. Please bear this in mind when planning and deploying locations.

Division Preference and Settings

Division preferences enable advanced customization of divisions on an individual basis.

Running a Division Preference

Note

There are no division preferences in this release of the system.

Customer Preference and Settings

Tool	Description	Impact and Limitations of Tool
AllowCrossClusterLogin	Allow Roaming User to login across locations.	The BVSMUserRoaming preference must be enabled at Provider level.
AllowFreeTextPickupGroupPilot-Number	Allow Free Text Pickup Group Pilot Number.	<p>Determines whether the free text pilot number is displayed when adding/modifying a pickup group. Select the required option from the drop-down:</p> <ul style="list-style-type: none"> • Derived from Provider - the value of the provider setting <i>FreeTextPickupGroupPilotNumber</i> is used to determine whether the free text pilot number feature is displayed or not. • Enabled - the provider level preference setting <i>FreeTextPickupGroupPilotNumberAdminRoles</i> is used to determine whether the logged in administrator user can use the free text pilot number feature. • Disabled -the free text pilot number feature is not displayed for that customer.
AllowRoamingMultiLogin	Allow Roaming User to login to multiple phones simultaneously.	Restricted to phones within the same cluster.

Tool	Description	Impact and Limitations of Tool
AllowSelfCarePINResetNoPrevious	Allows Self Care End User to reset their Voicemail and Extension Mobility Pin without having to provide the previous Pin.	When the preference is enabled the End User in Self Care is no longer prompted to provide the current PIN when resetting their Phone PIN. When the preference is disabled the End User in Self Care is prompted to provide the current PIN when resetting their Phone PIN.
AutoFeatureCustomer	Feature Group for Phone based registration (unless over-ridden by Location preference).	-
AutoLastResortFeatureCustomer	Feature Group for Last Resort Phones (unless over-ridden by Location preference).	-
AutoMoveCustomer	Allow Auto Move of Phone to locations (unless over-ridden by Location preference).	-
AutoRegisterLowestCustomer	Lowest allowed extension number for Phone based Auto registration (unless over-ridden by Location preference).	-
CustomerDefaultLoginPassword	Use the default password to reset user passwords.	-
EnableUniquenessIndicator	Enable Uniqueness to naming of IPT entities.	If this setting is enabled, the Location ID is appended to the device pool name for a 'Custom' device pool. The setting is named generically to allow future uniqueness indicators to use the same preference setting.
EndUserNamesAllNumeric	Require UserName to be all numeric.	Can only be set when there are no end users linked to the customer with existing alpha-numeric usernames. If set, a message ('Only numeric strings allowed') is displayed with the username field when a new end user is added to a location associated with the customer.
ForceOldRoamingLogoff	Force Roaming logoff (on old phone) if user logs in elsewhere.	The AllowRoamingMultiLogin preference (see above) must be disabled.
HuntGroupCallFwdCOS	COS to be used when setting Call forward for Hunt groups.	-

Tool	Description	Impact and Limitations of Tool
RoleLoginRequirePIN	Require entry of PIN during Role Login style Auto Registration.	-
ShowCorporateDir	Display Corporate Directory on phones.	-
ShowCorporateDir-Unreg	Display Corporate Directory on Unregistered phones.	-
ShowPersonalDir	Display Personal Directory on phones.	-
ShowSpeedDials	Display SpeedDials on phone.	-
UniqueEndUserEmailRequired	Ensures that end users have a valid and unique email address.	<p>By default, this preference is set to true, hence all end users within the system are required to have a unique email address. If your organization does not have this requirement, setting this preference to false disables end user email address validation within the system.</p> <p>Note: Certain Voicemail servers require all users to have unique email addresses. Please ensure your system is not affected by such limitations prior to disabling this preference.</p>
UseUserNameAsVMBoxNum	Use UserName as voicemail box number.	-
XML-CallForwardAll	Allow CallForwardAll editing via the Services menu.	-
XML-CallForwardBusy	Allow CallForward-Busy editing via the Services menu.	-
XML-CallForwardNoAnswer	Allow CallForward-NoAnswer editing via the Services menu.	-
XML-DirDisplayForLocalLocation	Rule to use for displaying Directory Numbers for Users in the Local Location.	The following display rules are available: Extension Number, Inter-site Number, Local PSTN Number, Local PSTN Number with Area Code, Full PSTN Number, Diallable Local PSTN Number, Diallable Local PSTN Number with Area Code, Diallable Full PSTN Number.

Tool	Description	Impact and Limitations of Tool
XML-DirDisplayForRemoteLocation	Rule to use for displaying Directory Numbers for Users in the Remote Location.	The following display rules are available: Extension Number, Inter-site Number, Local PSTN Number, Local PSTN Number with Area Code, Full PSTN Number, Diallable Local PSTN Number, Diallable Local PSTN Number with Area Code, Diallable Full PSTN Number.
XML-PhoneAutoRegistration	Displays Phone Auto Registration option on the Services menu. Refer to the AutoRegister section in the AutoCCMNewPhone Feature Guide for more details.	Note: Before making use of this functionality, disable the Location's <i>AutoRegister</i> preference, otherwise AutoCCMNewPhone automatically auto-registers the phones. Determines if the auto register provisioning option is displayed.
XML-PhoneBasedLanguageSelection	Display Phone Based Language Selection option on the Services menu.	-
XML-PhoneBasedProvisioning	Display Phone Based Provisioning option on the Services menu. Refer to Phone Based Registration on page 788 for more details.	Determines if the phone based provisioning option is displayed.
XML-PhoneLastResort	This functionality sets the phone up as the phone of last resort.	Determines if the phone last resort option is displayed. This registers the phone with the following details: <ul style="list-style-type: none"> <i>FeatureGroup</i> = the feature group defined in the preferences <i>AutoLastResortFeatureCustomer</i> or <i>AutoLastResortFeatureLocation</i> <i>Extension</i> = fixed to the last extension in the location based on the dial plan rules starting with '9'. For example a extension length of '4' would be 9999, or extension length of 3 would be 999. Note: This cannot be used if the number construction rules are setup for variable length fints. The transaction fails with an error if attempted with this rule.

Tool	Description	Impact and Limitations of Tool
XML-RoleLoginRegistration	Display Phone PIN Registration option on the Services menu.	This functionality initiates an Auto Register transaction followed by a user login transaction. The service either requests the pin or not depending on the customer preference <i>RoleLoginRequirePIN</i> (on = asks for the pin, off = no pin is required). This ultimately leaves the phone registered with the next available extension according to auto-register rules as well as the user logged into the phone.
XML-SetCallFwdPerLine	Allow Call Forward settings to be applied per Line.	-
XML-SingleNumberReach	Displays Single Number Reach option on the Services menu.	Shows a summary of existing remote destinations (if any). End users can manage the following remote destination fields: <i>Remote Name</i> , <i>Remote Number</i> , <i>Enable Mobile Connect</i> and <i>Selected Lines</i> . Note: The <i>Single Number Reach Support</i> checkbox must be selected (enabled) for the Location, and the end user must belong to a feature group that supports Single Number Reach in order to be able to use the SNR functionality on their phone.

Reseller Preferences and Settings

Reseller preferences enable advanced customization of resellers on an individual basis.

Running a Reseller Preference

Note

There are no reseller preferences in this release of the system.

System Preference and Settings

Tool	Description	Impact and Limitations of Tool
AllowPGWexport	Allows a system user to export PGW data to an MML file.	-
AllowTransactionReplay	Allow Transactions to be replayed from the transaction inquiry GUI screen.	Only super-users are able to access the transaction replay functionality.

Tool	Description	Impact and Limitations of Tool
AnyUserAnyPhone	Allows a user to login to any phone not just to the phones belonging to their customer.	<p>When <i>AnyUserAnyPhone</i> is <i>not</i> selected, the user and the phone must be in the same customer for the user to log in on the TUI.</p> <p>When <i>AnyUserAnyPhone</i> is selected, the phone and the user customer are no longer tied and the user might be from another customer. For a user to log in on a phone, the typed name on the TUI should then be the full username.</p>
AuditTransactions	Enable/Disable Transaction Auditing for the system.	It is normal for transactions to take longer to process when auditing is enabled compared to when auditing is disabled, this is due to the added processing steps required by the auditing functionality.
AutoCCMNewPhoneProvider	Select the default Provider for new phones automatically added to inventory.	-
CCLinePrefix	Contact Center Line Prefix.	This setting determines the prefix added to the line description in the IPPBX for when the Feature Group line setting <i>Contact Center Agent Line</i> is enabled. The default value is 'CC_Line'. If an admin user attempts to change the value to be blank, then the system still saves the value as 'CC_Line'.
ConfirmOnDelete	When this preference setting is selected (enabled), a confirmation box is displayed when the entity that the user selects to be deleted is being deleted. When entities other than the entity selected by the user to be deleted are cascade deleted (for example when an extension mobility profile with a dedicated line is deleted and the user's voice mail account, that is dependent on this dedicated line, is cascaded deleted in addition to what the user has selected to do) then a cascade delete confirmation dialogue box is displayed even if this preference setting is not selected (disabled).	Activating this option is highly recommended, however, please note that a user is presented with a confirmation dialog whenever the deletion of selected data is requested.

Tool	Description	Impact and Limitations of Tool
DefaultCustomerTimeZone	Use the default Customer Timezone.	-
DefaultDivisionTimeZone	Use the default Division Timezone.	-
DefaultLocationTimeZone	Use the default Location Timezone.	-
DefaultLoginPassword	Use the default password to reset user passwords.	-
DefaultProviderTimeZone	Use the default Provider Timezone.	-
DefaultResellerTimeZone	Use the default Reseller Timezone.	-
DefaultVoicemailPassword	Use the default password to reset voicemail passwords.	-
DeviceGroupName	Define the name used to refer to Device Groups.	-
InsecurePasswords	Use the insecure strategy of storing user passwords to cope with the technical limitations of some vendor products.	-
LogonBanner-da	Danish language text to display on the log on screen.	-
LogonBanner-de	German language text to display on the log on screen.	-
LogonBanner-default	Default text to display on the log on screen - unless language specific text is given.	-
LogonBanner-en	English language text to display on the log on screen.	-
LogonBanner-en-us	English (US) language text to display on the log on screen.	-
LogonBanner-es	Spanish language text to display on the log on screen.	-
LogonBanner-fr	French language text to display on the log on screen.	-
LogonBanner-ga	Irish language text to display on the log on screen.	-
LogonBanner-nl	Dutch language text to display on the log on screen.	-
SystemShowTimeZone	Select system default time zone for displayed times.	-
TransitDefer	Number of transit switch transactions to process as a single unit.	-
UsePerLineCoS	Use per-line class of service (CoS).	Applies to phone registration, phone management and user mobility profiles.

Building Preferences

Procedure

To edit the preferences for the selected building:

- Step 1** Select the building *Name* (active text link) of the building that you would like to modify.
- Step 2** Click the **Preferences** button.
- Step 3** Click the **Building Preferences** button.

A list of all relevant preferences is displayed, this list includes the name and a description for the preferences. Currently, only the *AutoDevicePoolAllocation* preference setting is available. To enable or disable this preference setting:

- a** Select the *AutoDevicePoolAllocation* (active text link) preference that you would like to enable or disable.
- b** To disable the preference, de-select the *Current Setting* checkbox.
- or**
- c** To enable the preference, select the *Current Setting* checkbox.

- Step 4** Click the **Modify** button.
-

The preference is updated for the building.

Procedure

Default Customer Preferences

To edit the default customer preferences for the building:

- Step 1** Select the building *Name* (active text link) of the building that you would like to modify.
- Step 2** Click the **Preferences** button.
- Step 3** Click the **Default Customer Preferences** button.

A list of all the relevant preferences is displayed, this list includes the name and a description of the preferences. To enable or disable a particular setting:

- a** Select the *Preference Name* (active text link) of the preference you would like to enable or disable.
- b** To disable the preference, de-select the *Current Setting* checkbox.
- or**
- c** To enable the preference, select the *Current Setting* checkbox.

- Step 4** Click the **Modify** button.
-

The preference is updated.

Procedure

Default Location Preferences

To edit the default location preferences for the building:

- Step 1** Select the building *Name* (active text link) of the building that you would like to modify.
- Step 2** Click the **Preferences** button.
- Step 3** Click the **Default Location Preferences** button.

A list of all the relevant preferences is displayed, this list includes the name and a description of the preferences. To enable or disable a particular setting:

- a** Select the *Preference Name* (active text link) of the preference you would like to enable or disable.
- b** To disable the preference, de-select the *Current Setting* checkbox.
- or**
- c** To enable the preference, select the *Current Setting* checkbox.

- Step 4** Click the **Modify** button.
-

The preference is updated.

Dial Plan Preference and Settings

Tool	Description	Impact/Limitations of tool
Internalpublishednumber	Dial plan allows definition of Internal published number for location.	-
PSTNpublishednumber	Dial plan allows definition of E164 published number for location.	-

Operations Tools

Operations Tools allow for the automation of multi-step processes, such as de-registering all phones in a location.

The operations tools are typically used for testing purposes, when a 360 degree test needs to be performed, such as adding a location, deleting a location and then adding the same location again. They are also very useful for refreshing a location when adding a new dial plan to legacy locations.

Operations tools are only available to Provider administrators (or higher).

Note

While running operations tools, you can perform other tasks within the system.

The following operation tools are available:

Operation Tools	Description	Remarks
Location Level		
Logout all end users of a location from phones at that location.	This tool is very similar to <i>Logout all roaming end users at location from all phones</i> (see below) except that it is used for logging out users logged in using Unified CMs extension mobility feature as opposed to CUCDMs <i>BVS-MUserRoaming</i> . For this to function correctly, the Provider preference <i>BVS-MUserRoaming</i> must be disabled (not selected).	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Logout all roaming end users of a location from all phones.	Logs out all roaming end users in a location from their phones.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Re-apply feature group capabilities for a given location	Re-applies feature group capabilities for a given location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the Feature Group from the drop-down list then click the Re-apply button once you are sure you would like to proceed.</p>
Refresh All Phone Features at a location	This operation re-syncs the system and the Cisco Unified Communications Manager (Unified CM) data. This operation assumes that the system is the master.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Activate Locations	Used to connect locations. This tool enables administrators to fully configure a location prior to the locations deployment. Route and Translation patterns can also be added for the location. For more information, see the Connect Location online help section.	<p>Click the Activate button adjacent to the Location that you would like to activate. Enter the relevant <i>Pattern</i> (the value entered here will be substituted for #CLOCPATTERN in the models), and <i>Model name suffix</i> (from the drop-down menu) as required and click Activate. These fields are only available if matching models are found.</p> <p>To add AutoRegistered Phones to a locations pickup group, select the <i>Pickup Group</i> active text link adjacent to the relevant Location.</p>

Operation Tools	Description	Remarks
Location Level		
Delete All SpeedDials from Users at Location	Deletes all speed dials from users at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Busy Lamp Fields from Users at Location	Deletes all busy lamp fields from users at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Pickup Groups at Location	Deletes all pickup groups at a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Presence at Location	Deletes all presence at a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Disassociate all E164 numbers in use at a location	Disassociates all E164 numbers in use at a particular location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete All Number Groups at Location	Deletes all number groups at location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Delete All Roaming profiles at Location	Deletes all roaming profiles at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Users at Location	Deletes all users at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Release all usage of Billing Codes by users at a location	Releases all billing codes being used by users at a location. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete All Call Parks at Location	Deletes all call parks at location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Suspend All Phones At Location Out of Service	Suspends all phones (or the first line only of all phones) at a location that are out of service.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>Note</p> <p>Make sure that you select the <i>First Phone Line Only</i> checkbox if you want to suspend the first phone line only of all phones.</p> <p>After selecting the tool's active text link, click the Suspend button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Suspend All Extension Mobility Profiles At Location Out of Service	Suspends all extension mobility profiles at a location that are out of service.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Suspend button once you are sure you would like to proceed.</p>
Release All Console Services From A Location	Releases all console services from a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Add Autoregistered Phones to pickup group	Adds all Autoregistered Phones to the specified pickup group.	After selecting the tool's active text link, select the required <i>pickup group</i> from the drop-down list then click the Submit button once you are sure you would like to proceed.
Delete All Adjacent Area Codes at Location	Deletes all adjacent area codes at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Directed Call Parks at Location	Deletes all directed call parks at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all CTI Devices in the location	Delete all CTI Devices in the location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Bulk Apply Voicemail Profiles	Bulk Apply Voicemail Profiles.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the voicemail profile that you would like to move users from in the <i>Change from</i> profile list. Next, select the voicemail profile that you would like to move users onto from the <i>Change to</i> profile list, then click the Submit button once you are sure you would like to proceed.</p>
Delete all Single Number Reach Destinations at Location	Deletes all Single Number Reach Destinations from a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Logout all roaming users of a location from all phones at location	Logs out all roaming users in a location from all phones at the location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Logout all roaming end users at a location	Logs out all roaming end users at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Refresh All End Users at a location	This operation will re-sync the system and the Unified CM data. This operation assumes that the system is the master.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Refresh All Mobility features at a location	This operation will re-sync the system and the Unified CM data. This operation assumes that the system is the master.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Disable activation of Billing Codes assigned to a location	Disables activation of billing codes assigned to a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete All SpeedDials from Phones at Location	Deletes all speed dials from phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Busy Lamp Fields from Phones at Location	Deletes all busy lamp fields from phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All Hunt Groups at Location	Deletes all hunt groups at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete Orphaned Presence at Location	Deletes all Orphaned Presence instances at a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Release all unassociated E164 numbers assigned to a location	Releases all unassociated E164 numbers that are assigned to a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete All Voicemail accounts at Location	Deletes all voicemail accounts at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
UnRegister All Phones at Location	De-registers all phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Release All Phones at Location	Releases all unregistered phones at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Release all usage of Billing Codes assigned to a location	Releases all usage of billing codes assigned to a particular location. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Release all usage of Authorization Codes assigned to a Location	Releases the usage of all authorization codes assigned to a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Unsuspend All Phones At Location Out of Service	Unsusponds all phones at a location that are out of service.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Unsuspend button once you are sure you would like to proceed.</p>
Unsuspend All Extension Mobility Profiles At Location Out of Service	Unsusponds all extension mobility profiles at a location that are out of service.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Unsuspend button once you are sure you would like to proceed.</p>
Release All Console Operators From A Location	Releases All Console Operators From A Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Apply Domain Name to Android devices	Applies a new domain name to all registered Cisco Dual Mode for Android devices.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the Apply button once you are sure you would like to proceed.</p>
Release All PSTN Ports From Location	Releases all PSTN ports from a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete All VLAN at Location	Deletes all VLANs at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Delete All IP PBX translation patterns at Location	Deletes all IP PBX translation patterns at a location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete All lines from number groups in linked locations	Deletes All lines from the number groups within linked locations.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Update All Phone/Extension Mobility/CTI Line Masks At Location	<p>This function updates all phone/extension mobility/CTI line masks at a specified location.</p> <p>Note</p> <p>If there are registered phones, configured extension mobility profiles, configured CTI devices, or registered analog ports in the location, and E164 numbers are then associated to the internal number/s, or if a PSTN published number is either added/modified or deleted at the location, then run this Ops tool to update the relevant line mask/s at the location.</p>	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Delete All Service URL buttons for Phones at Location	This function deletes the Service URL Buttons from the Roaming Profile for End Users at a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the Delete button once you are sure you would like to proceed.</p> <p>Note</p> <p>This operation is useful when an administrator is trying to delete a user-level IP Phone service. Before the service can be deleted, all Service URL button assignments must be removed for this service.</p>
Delete All Service URL buttons for Users at Location	This function deletes all Service URL buttons for users at a Location.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the Delete button once you are sure you would like to proceed.</p> <p>Note</p> <p>This operation is useful when an administrator is trying to delete a user-level IP Phone service. Before the service can be deleted, all Service URL button assignments must be removed for this service.</p>
Update All Phone/Mobility/CTI Line Masks At Location	This function will check all the devices at the location and re-provision any that are found to have out-of-date line masks by running a modification on them.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the Submit button once you are sure you would like to proceed.</p> <p>Note</p> <p>The Ops Tool does not explicitly update line masks for SNR Remote Destination lines as it will update the devices to which these lines are associated if necessary.</p>
Device Groups		

Operation Tools	Description	Remarks
Location Level		
Destroy a Device Group and delete its resources (all phones/users etc)	This operation will destroy a Device Group and delete all of its resources (including all phones/users etc.).	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Delete all Device Groups at Location and release their resources	Delete all Device Groups at Location and release their resources.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Division Level		
Re-apply feature group capabilities for a given division	Re-applies feature group capabilities for a given division.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the <i>Feature Group</i> from the drop-down list then click the Re-apply button once you are sure you would like to proceed.</p>
Release all usage of Billing Codes assigned to a division	Releases all usage of billing codes assigned to a division. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Macro Level processes for Operations (CAUTION: Please Use with care!!)		
Destroy a location (all phones/users etc)	<p>Note</p> <p>Phones are effectively unassigned from the 'destroyed' location and placed back into the phone inventory at Division level, where they can be assigned to another user/location.</p> <p>Destroys a location, as well as all of the locations phones, users etc.</p>	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Customer Level		

Operation Tools	Description	Remarks
Location Level		
Release all usage of Billing Codes assigned to a customer	Releases all usage of billing codes assigned to a customer. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the <i>Feature Group</i> from the drop-down list then click the Re-apply button once you are sure you would like to proceed.</p>
Suspend All Phones Under Customer Level	Suspends all phones under the customer level.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Suspend button once you are sure you would like to proceed.</p>
Release All PSTN Ports From Customer	Releases all PSTN ports from a customer.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Move button once you are sure you would like to proceed.</p>
Re-apply feature group capabilities for a given customer	Re-applies feature group capabilities for a given customer.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, select the <i>Feature Group</i> from the drop-down list then click the Re-apply button once you are sure you would like to proceed.</p>
Unsuspend All Phones Under Customer Level	Unsusponds all phones under the customer level.	After selecting the tool's active text link, all phones under the customer level will be unsuspended.
Set Customer Codecs	Sets the Customer Codecs for the Intra-Location Max Audio Bit Rate and the Inter-Location Max Audio Bit Rate.	<p>Use the drop-down lists to select the <i>Intra-Location Max Audio Bit Rate</i> and the <i>Inter-Location Max Audio Bit Rate</i> then click the Submit button.</p> <p>Note</p> <p>If a customer has multiple clusters, the provisioning for this is done on all the clusters.</p>
Macro Level processes for Operations (CAUTION: Please Use with care!!)		

Operation Tools	Description	Remarks
Location Level		
Destroy a division (ALL locations in it)	Destroys a division and all locations in it.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Reseller Level		
Release all usage of Billing Codes assigned to a reseller	Releases all usage of billing codes assigned to a reseller. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Macro Level processes for Operations (CAUTION: Please Use with care!!)		
Destroy a customer (All divisions in it)	Destroys a customer all divisions in it.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Destroy a building (All locations in it)	Destroys a building and all locations in it.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
Provider level tools		
Delete all E164 numbers inventory for a Provider	Deletes all E164 numbers in the inventory for a provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Delete all IP Subnets inventory for a Provider	Deletes all IP Subnets inventory for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>Only subnets that are not in use will be deleted. Perform the OpsTool <i>Unregister all phones at Location</i> to release the subnets so they can be deleted using the <i>Delete all IP Subnets inventory for a Provider</i> OpsTool.</p> <p>After selecting the <i>tool's</i> active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all Phone Inventory for a Provider	Deletes all Phones in the inventory for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>Only phones that are not registered will be deleted. To unregister phones first, the OpsTool <i>Unregister all phones at Location</i> can be performed before performing the <i>Delete all Phone Inventory for a Provider</i> OpsTool.</p> <p>After selecting the <i>tool's</i> active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all Billing Codes inventory for a Provider	Deletes all billing codes in the inventory for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all Authorization Codes for a Provider	Deletes all authorization codes for a provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Release All PSTN Ports	Releases all PSTN ports.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>

Operation Tools	Description	Remarks
Location Level		
Delete all Feature group templates defined for a Provider	Deletes all feature group templates defined for a provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all Hardware Groups defined for a Provider	Deletes all Hardware Groups defined for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Delete all Associated Device definitions for a Provider	Deletes all associated device definitions for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Release all usage of Billing Codes assigned to a provider	Releases all usage of billing codes assigned to a provider. Billing codes that are assigned but not enabled will be ignored by these opstools.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Release all Authorization Codes for a Provider	Releases all authorization codes for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Submit button once you are sure you would like to proceed.</p>
Delete all PBX templates defined for a Provider	Deletes all PBX templates defined for a Provider.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Delete button once you are sure you would like to proceed.</p>
Macro Level processes for Operations (CAUTION: Please Use with care!!)		

Operation Tools	Description	Remarks
Location Level		
Destroy a reseller (ALL customers in it)	Destroys a reseller and all customers related to that reseller.	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>
System Level		
Set Dial Plan Codecs	Sets the system level codecs for Intra-Location Max Audio Bit Rate and the Inter-Location Max Audio Bit Rate.	Use the drop-down lists to select the <i>Intra-Location Max Audio Bit Rate</i> and the <i>Inter-Location Max Audio Bit Rate</i> , select the <i>Customer/Building Codec Configurable?</i> checkbox if you would like customers to be able to select their own codecs, then click the Submit button.
Macro Level processes for Operations (CAUTION: Please Use with care!!)		
Destroy a provider (ALL resellers in it)	Destroys a provider and all resellers related to that provider	<p>Note</p> <p>This function is disruptive to end users making phone calls.</p> <p>After selecting the tool's active text link, click the Destroy button once you are sure you would like to proceed.</p>

Upgrade Limitations

The following are known limitations when upgrading from an older version of the system to the latest version of the system:

- Validation functionality was improved in system release 7.1 to ensure that leading and trailing spaces are not committed to the system's database. No migration script is provided to remove leading and trailing spaces from data that is already stored in the system's database or on the network devices provisioned by the system.
- The *FwdRedirectingExternalNumonCallFwd* setting, under *Advanced Provider Telephony Settings*, is disabled by default when a system is migrated from an older version of the system that did not have this functionality. This setting can be changed after migration as required.
- If you are migrating from a version prior to system release 7.1.1, during the migration process the Alerting Name feature will automatically be enabled in the relevant feature group and a default alerting name consisting of the extension number will automatically be registered.
- When migrating to system release 7.1.1 R4 or above, administrators may experience compatibility issues with certain branding files. This compatibility issue only relates to the exportation, importation and modification of brands. All brands currently in use will continue working unaffected once system release 7.1.1 R4 or above has been applied. If you experience difficulties with branding, please contact system support and they will be able to update your Pre-R4 branding files.

Note

All brands created using the brand editor after system release 7.1.1 R4 is applied will not be affected.

- With the auto attendant functionality prior to system release 7.1 SP 4, it was possible to create an Auto Attendance (AA) service without linking it to a Voicemail Service (VM). This association was performed indirectly based on the common location. Starting with system release 7.1 SP4, it is now mandatory to link AA services to a VM service. Certain upgrade and migration scripts will fail if there are AA services that are not associated with a VM service. To avoid this, the system provides a script to verify that all AA services are associated to a VM service. If any erroneous AA services are identified, browse to the affected AA service and specify a VM service. The SQL script to run is:

```
SELECT aa.providername, aa.resellername, aa.companyname,
aa.autoattendant servicename, aap.autoattendant servicename
from autoattendant service AS aa
LEFT JOIN autoattendant service_pilot aap
ON (aa.providername = aap.providername
AND aa.resellername = aap.resellername
AND ((aa.building_id IS NULL AND aa.companyname =
aap.companyname)
OR (aa.building_id IS NOT NULL AND aa.building_id =
aap.building_id))
AND aa.autoattendant servicename = aap.autoattendant servicename)
WHERE aap.autoattendant servicename IS NULL;
```

Unified CM Group Allocation Logic

Overview

When adding a location, and using Typical for Device Pool Configuration, CUCDM selects the Unified CM Group for the location based on the Stream availability of the groups within the selected cluster.

This logic behind this workflow is:

- CUCDM calculates the Stream availability on each Unified CM group marked for Phones within the selected cluster.
- Streams available is calculated by subtracting the Used Streams from the Maximum Supported Streams.
- CUCDM then selects the group with the most Streams available.

Note

The capacity of a Unified CM Group is a configurable setting within CUCDM. Groups are managed within the CUCDM's interface by browsing to *Network > PBX Devices*, selecting the required Unified CM then clicking the *Groups* button.

Note

If there is no group with sufficient spare capacity available when attempting to add a location, the error message returned is: *No 'group' with sufficient resources available on PBX, please check 'groups' within your PBX device [ccmclustername]*. If you exceed the available streams by allocating more Streams to the Device Pools than are available in the Group, the error message returned is: *Allocated supported streams exceeds the available streams*.

Adding a New CCM Group to the Cluster

When a new Unified CM Group is added to a cluster, the load and allocations within the existing groups are not affected. However, the new group will be used for any new locations added to the CUCDM if its Available Streams are greater than, the existing groups.

Caveats and Limitations

Please note the following points regarding Unified CM Group allocation logic:

- Adding a new Unified CM Group to a cluster does not change the existing load or allocation to the other groups.
- Streams used is based on the number of Streams Allocated to Device Pools and not the number of lines, phones or extensions.

Glossary

See the following table for a list and description of commonly used, acronyms, abbreviations and terms:

Term	Description
1ESS	Number 1 Electronic Switching System
1FR	Flat rate service
2 5G	Enhanced 2G mobile telephone
2G	Second generation mobile telephone
3G	Third generation mobile telephone
4WTS	Four-wire termination set
A number	Calling number
ACD	Automatic Call Distribution - Director
ACTS	Advanced Coin Telephone Service
ADSL	Asymmetric Digital Subscriber Line
AMA	Automatic Message Accounting
ANI	Automatic Number Identification
API	Application programming interface
Associated	An associated phone is linked to a user, who becomes associated with the Phones telephone number.
Auto Attendant	An automated attendant or auto attendant system transfers telephone calls to the extension of a user or department without the intervention of a receptionist or operator. This is achieved via a system of voice menus that the person initiating the call interacts with via their telephone keypad or via voice commands. In some auto attendant systems, there are message-only information menus and voice menus that are used so that an organization can provide business information such as hours, directions to their premises, information about job opportunities, and answer other frequently-asked questions. After the message has played, the caller can be forwarded to the receptionist or they can return to the main menu.
AXL	AVVID XML layer
B number	Called number
BOK	Unblocking
CC	Country code
CCIS	Common Channel Interoffice Signaling
CDRs	Call Data Records
CEPB	Communications Enabled Business Processes
CF	Call forward

Term	Description
CID	Caller ID
Cisco	Cisco is the leading supplier of IP equipment, including IP Telephony. Their history as the pre-eminent experts on IP has enabled them to compete effectively with the traditional voice vendors, who have had to make the transition to data.
Cisco36xx	A Cisco 36xx Series Router
Cisco Emergency Responder	A Cisco Emergency Responder (Emergency Responder) server ensures that the Cisco Unified Communications Manager (Unified CM) sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates equipment moves and changes.
Cisco Unified Presence	Cisco Unified Presence (Unified Presence) is a standards-based platform that collects information from multiple sources about user availability and communications capabilities to provide rich presence status and facilitate presence-enabled communications with Cisco Unified Communications and other critical business applications.
Cisco SRST	Cisco Secure Survivable Remote Site Telephony, a disaster mitigation technology.
CLI	Command-line interface or Caller ID - Caller Line Identification
CLID	Caller ID - Caller Line ID
CLIP	Calling Line Identification Presentation
CLIR	Calling line identification restriction
Cluster ID (CID)	This is an ID assigned to each Cisco Unified Communications Manager PBX cluster in the system. This is configurable when adding the cluster and can be viewed on the cluster details page.
Contact Center	A Contact Center is a hardware and software solution that involves the intelligent routing of all contacts, call treatment, and general contact management over a multichannel IP infrastructure. Contact Centers often contain functionality to enable automatic call distribution functionality that interfaces with an organizations unified communications solution.
CoS	Class of service
COSMOS	Wire records
CPID	Call processing identifier (unique system-wide). First part of the FINT. The CPID and RID need to be unique within a provider. This is assigned to hardware as required (e.g. PBX, PGW, Voicemail, etc). The CPID is generally configurable when adding the hardware and is displayed when viewing the settings.
CSP	Communications Service Provider
CSS	Calling search
CT	Call type
CTI	Computer telephony integration, also called computer-telephone integration or CTI, is technology that allows interactions on a telephone and a computer to be integrated or co-ordinated. As contact channels have expanded from voice to include email, web, and fax, the definition of CTI has expanded to include the integration of all customer contact channels (voice, email, web, fax, etc.) with computer systems.
CUCDM	Cisco Unified Communications Domain Manager. Also commonly referred to as the "system".

Term	Description
Dial plan	A dial plan establishes the expected number and pattern of digits for a telephone number, including country codes, access codes, area codes, extension numbers and all combinations of digits dialed. Dial plans must comply with the telephone networks to which they connect.
DDCO	Direct Dial Central Office (Opposite of DID)
DDD	Direct Distance Dialing
DDI	Direct Dial Inward (same as DID)
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol - Used to perform basic configuration of computer systems, usually at boot time. May be used to set network parameters such as IP address, subnet mask and host name.
Dialplan	Defines the number construction rules
DID	Direct Inward Dialing (US term for DDI).
DMS	Digital Multiplex System
DN	Directory Number
DNIS	Dialed Number Identification System
DP	Dial plan
DPCODE	Dial Peer Code
DPNSS	Digital Private Network Signaling System.
DSL	Digital Subscriber Line
DTMF	Dual-tone multi-frequency. A method for instructing a telephone switching system of the telephone number to be dialed. This is done by sending pairs of tones down the line.
E164	ITU-T recommendation defining PSTN numbering plan E164.
E164 Numbers	E164 numbers must always be unique and the local PTT should ensure that the same number ranges are not given out twice.
EDRs	Event Data Records
EISUP	Extended ISDN user part
ELIN	Emergency Location Identification Number
EOL	End of line (variable used by the system to determine the end of line in each model).
EXT	Extension and external prefix
EXTN	Extension Final part of the FINT
FDM	Frequency-division multiplexing
FINT (fint)	The full Internal Number, CPID + RID + SLC + EXTN = Cisco Unified CM DN. This is the full internal number the system knows the lines as. The construct of this is defined in the number construction rules. When a location is added, the full fint inventory is created for the location.
FNN	The full national number (PSTN number). The E164 telephone number without area code
GK	Gatekeeper
Glassfish	Open Source Application Server
GPRS	General Packet Radio Service
GSM	Global system for mobile communications

Term	Description
GUI	Graphical user interface
GW	Gateway
H 323	ITU - T umbrella recommendation defining audio-visual protocols on a packet network H323 Protocol.
H - M-UCS	Hosted - Managed-Unified Communications Solution
HSI	H323 Signaling Interface
Hunting	Hunting or a hunt group is a telephony concept that refers to the concept of distributing phone calls from a single telephone number to several phone lines. A number of different hunt methods exist that can be configured depending on the organizations needs and requirements. The most common hunting methods include multi-line hunting, linear hunting, circular hunting and most-idle hunting.
Hunt Group	See the term Hunting
ICPID	Call processing identifier, IPPBX-based
IDDD	International Direct Distance Dialing
Idle URL	An Idle URL can be seen as a form of advanced screensaver. When a phone has been not received user input for a configurable amount of time (URL Idle Time Parameter), the system will perform a HTTP GET for the URL in the URL Idle field and will then display the contents of the URL on the phones screen. This content can be anything from an organizations logo to more advanced data such as a weather forecast or company updates.
ILEC	Incumbent Local Exchange Carrier
IM	Instant messaging
IMACS	IMACs stands for Installs, Moves, Adds and Changes. It covers the administration for: Installing new Customers, Locations, Users and Phones; moving Users and Phones; Adding Users and Phones and changing the Features and Services used for Users and Phones.
IOS	Internetwork Operating System is an operating system from Cisco that is the primary control program used on Cisco Routers and devices. IOS is widely used and is robust system software that supports the common functions of all products under Cisco's CiscoFusion architecture.
IP	Internet Protocol
IP Addressing	IP Addressing should be unique, however, where two Customers have chosen the same private IP address ranges for their locations, NAT will be required to ensure that IP addresses within the system are unique.
IPT	Internet Protocol Telephony (IP Telephony)
ISC	The Cisco IP Solution Center (ISC). A security management solution from Cisco.
ISD	International Subscriber Dialing
ISDN	Integrated Services Digital Network
ISP	Inter-site prefix
ISUP	ISDN user part
ITU-T	International Telecommunications Union - Developer of global info-communications standards
IVR	Interactive voice response

Term	Description
Inventory	When a phone is initially entered into the system, it is added as an inventory item in the Service Providers warehouse. The Device Name and type are the only things known about this Phone. Over time, the phone will be allocated initially to a Reseller, who in turn will allocate it to a Customer. It is still an inventory item. It does not become a provisioned phone until it has been allocated to a Location.
LEPN	Location Emergency Published Number
Location Name	The Location name must be unique within a Customer. A naming convention is recommended, where a suffix is added to the location name that contains a reference to the Customer, for example, nsydney_cisco, Location names can be re-used within different Customers.
Logged on	Only a phone that has Extension Mobility Support can be logged onto by a user using a User Mobility profile. Once logged-on, the phone adopts the profile of the Mobile User and drops their registered number and profile.
LRID	Routing identifier, location-based
MAC Address	A Media Access Control address (MAC address), is a unique identifier assigned to network devices by their manufacturers. They are used for identification and in the Media Access Control protocol sub layer. MAC addresses are unique by their very nature.
MDF	Main Distribution Frame
MF	Multi-frequency
MGCP	Media Gateway Control Protocol
MML	Man-machine language
MT	Multi-tenant
MWI	Message waiting indicator
NANP	North American Numbering Plan - a dial plan based on 3-digit area codes and 7-digit telephone numbers used by 24 countries in North America and the Caribbean.
NAT	Network Address Translation - A standard that enables a local area network (LAN) to use one set of IP addresses for internal network traffic and a second set of addresses for external traffic.
NGN	Next Generation Network
NOA	Nature of address
Netwise	A Netwise CMG Telephony Server
NTP	Network Time Protocol - used to synchronize computer system clocks to a high degree of accuracy.
OCS	Online charging system - A system allowing Communication Service Providers to charge their customers, in real time, based on service usage
OSS	Operations Support Systems
PABX	Private Automated Branch Exchange, often shortened to PBX.
PAT	Port Address Translation - A form of network address translation whereby each IP Address on the LAN is translated to the same IP address but each with a different port.
PBX	Private branch exchange PABX
PCC	Padded country code
PGW	PSTN Gateway

Term	Description
PGW Cisco Transit switch	The Cisco PGW (Protocol Gateway) is a multi-protocol, carrier-grade soft-switch designed to support media gateway control functions and interworking in next-generation networks (NGNs).
Phone MAC Address	See the MAC Address glossary entry for a full explanation of a MAC address. By their very nature, all Phone MAC addresses in the system are unique.
Pilot Number	A pilot number is an address or location within a PBX or IP-PBX and is generally defined as a blank extension number or an extension that does not have a person or telephone associated with it. Without a defined pilot number, the PBX or IP-PBX cannot locate where the incoming call was received. Pilot Numbers are used in the system for a number of services such as Hunt Groups and Voicemail services.
PMBX	Private Manual Branch exchange
POTS	Plain old telephone service
PRI	Primary Rate Interface
Provisioned	Once a phone has been moved into a Location and into a specific subnet, the system allocates an IP address to the phones MAC address. If that phone is physically connected to the correct VLAN in the Location, then it will be automatically provisioned with the allocated IP address.
Public Holiday	Public holidays are often referred to as Bank Holidays, National holidays, Federal Holidays and Vacations. Public Holidays are days that have been declared by a national, or sometimes local, authority to be non-working days. Public holidays are usually declared as an official observance of a religious, national, or culturally significant event. The impact on business is that businesses may be closed for business on days that would traditionally be trading days, for example Monday to Friday. Public holidays on days that are traditionally days of rest, tend to have a lesser impact on business.
PSTN	Public Switched Telephone Network
PTT	Push to Talk
QoS	Quality of Service
QSIG	Q Signaling (ISDN-based protocol for signaling between PBXs)
RCMAC	Recent Change Memory Administration Center
Registered	Only a provisioned phone can be registered. The registering process provides the phone with a telephone number and a configuration file. Only a registered phone can operate as a normal phone and can make and receive calls.
REN	Ringer equivalency number
ROI	Return on Investment
Routing ID (RID)	This is configurable as to whether it is a customer level or location level ID. Although it is configurable, if anything other than Location is selected you will likely have problems. This ID is selected for a location and is unique for the CPID. In the case of a location, the RID could be an available rid for the CPID of the IPPBX of the location.
SCCP	Skinny Client Control Protocol
SDP	Service Delivery Platform

Term	Description
Service Activation	Service activation is the technical process of creating, delivering and managing a service to - for a customer. It generally involves the configuration of multiple products (for example dial-tone, voice mail, conferencing, corporate directories and XML applications) for the one service.
SF	Single Frequency supervision tone (2600)
SIP	The Session Initiation Protocol (SIP) is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet.
Site Code	This is a location level code assigned for each location In the system, this would be required if you wanted more than a single location in the system (as the fint needs to be unique). The site code inventory is managed per customer in the system. The length of the site code is always allowed to be variable with a defined maximum length. Overlapping site codes are not allowed within a customer - if a site code of 1 was defined, then a site code of 12 would not be allowed.
SLC	Site location code (unique within a customer) Penultimate part of the FINT
SME	A Cisco Unified Session Manager Edition (Cisco SME) is a transit switch used to aggregate multiple unified communications systems, referred to as leaf systems.
SMS	Short Message Service or text messages
SNMP	Simple Network Management Protocol. A widely supported protocol used to manage, monitor and configure network devices.
SOAP	Simple Object Access Protocol
SP	Service Provider
SP Lock	Unlocking
SRST	Survivable Remote Site Telephony
SS7	Signaling System 7
STD	Subscriber trunk dialing
TAPI	Telephony Application Programming Interface
TCO	Total Cost of Ownership
T-CXR	T carrier
Technician Server	A server that is not managed by the system, but rather directly by a technician.
The system	A term used in the documentation to refer to the application and its related hardware and software components.
TOD	Time of day
TSPS	Traffic Service Position System
TXE	Telephone exchange Electronic
UAX	Unit Automatic exchange
UC	Unified Communications
UC SDP	Unified Communications Service Delivery Platform
UCaaS	Cisco's Unified Communication as a Services, for hosted and managed IP Telephony, offers a proven end-to-end integrated reference architecture for Unified Communications and IP telephony services, specifically targeting large, Enterprise and Service Provider deployments.

Term	Description
Unified CM	Cisco Unified Communications Manager
Unified Mobility	Cisco Unified Mobility
Unified Presence	Cisco Unified Presence
Unity	Cisco Unity is a powerful Unified Communications solution that provides advanced, convergence-based communication services such as voice and unified messaging on a platform that offers the utmost in reliability, scalability, and performance.
UnmanagedPBX	Unmanaged PBXs are often used as parent components for a location.
User Name	The Last Name and First name can be the same, but the User Name must be unique across all Customers. Hence, we recommend adding a domain suffix to user names, such as cmay_cisco_ns, where the suffix is an abbreviation for Cisco North Sydney location. Alternatively, the user name can be the same as the user phone number (DDI). This ensures that the user name is always unique.
VM	Voicemail
VOIP	Voice over Internet Protocol
WAP	Wireless Application Protocol
WATS	Wide Area Telephone Service
WTAI	Wireless Telephony Applications Interface
XML	Extensible Markup Language