Cisco Hosted Unified Communications Services Provisioning Guide Release 7.1(a)

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

Text Part Number: OL-23270-01

CONTENTS

Preface

This preface includes the following sections:

Overview

This guide describes how to use Vision OSS USM to provision the Cisco Hosted Unified Communications Services (UCS) core platform and components. This document is designed to be used in conjunction with *Getting Started with Cisco Hosted Unified Communications Services.*

Audience

This document is written for Cisco Advanced Services (AS), system integrators, Cisco partners, and Cisco customers who are interested in implementing Cisco Hosted UCS 7.1(a).

This document is to be used with the documentation for the individual components of the Hosted UCS 7.1(a) platform after completing the high-level design (HLD) and low-level design (LLD) for a specific customer implementation.

Organization

This manual is organized as follows:

(

Chapter 1, "Hosted UCS Call Routing and Dial Plans"	Describes how call routing occurs and how dial plan models work within a Cisco Multi-tenant Hosted Unified Communications Services (UCS) 7.1(a) deployment.
Chapter 2, "Hosted UCS Static Configuration"	Describes the static configuration required as part of the lab builds for Cisco Hosted Unified Communications Services (UCS), Release 7.1(a).
Chapter 3, "Defining and Configuring Core Network Elements and Resources"	Describes how to define and configure the core network elements required for implementing the Hosted Unified Communications Services platform.
Chapter 4, "Managing Countries and Provider Resources"	Describes how to define and configure other USM objects and resources, such as countries.
Chapter 5, "Managing Legacy PBX Support"	Describes how to integrate the Hosted Unified Communications Services platform with legacy PBX systems.
Chapter 6, "Provisioning Movius VoiceMail and Auto Attendant Services"	Describes the provisioning of Movius VoiceMail and Auto Attendant services and configuring SBC for the Movius Auto Attendant to work with PGW.
Chapter 7, "Provisioning the Local PSTN Breakout Support"	Describes how PSTN calls can be routed via Local Gateways in the Hosted UCS reference architecture for the Hosted UCS 7.1(a) Release.
Chapter 8, "Provisioning LBO Location with Cisco Emergency Responder"	Describes the deployment of Cisco Emergency Responder (CER) in the Hosted UCS 7.1(a) platform
Chapter 9, "Provisioning NAT/PAT Support"	Describes how to configure Cisco Hosted UCS components when IP phones are connected to the USM server through a Cisco NAT/PAT device.
Chapter 10, "Provisioning Other Hosted Unified Communications Services Features"	Describes how to use VisionOSS Unified Services Manager (USM) application to provision the components of the Cisco Hosted Unified Communications Services (UCS), Release 7.1(a) platform
Chapter 11, "Provisioning Analog Gateway"	Describes the Provisioning of analog VG224 gateway for a customer location in Hosted UCS Release 7.1(a).
Chapter 12, "Provisioning Linked Locations"	Describes how the New Linked Locations functionality on Hosted UCS 7.1(a) allows a single site code to be shared within a group of locations called linked locations..
Chapter 13, "Provisioning Single Number Reach"	Describes Single Number Reach (SNR) which provides Cisco Unified Communications users with the ability to be reached via a single enterprise phone number that rings on both their IP desk phone and their cellular phone (Remote Destination), simultaneously.

Appendix A, "Hosted Unified Communications Services Location Administration"	Describes the options available to Location-level administrators within the Hosted UCS Release 7.1(a).
Appendix B, "Hosted Unified Communications Services Division Administration"	Describes the options available to Division administrators within the Hosted Unified Communications Services (UCS) system.
Appendix C, "Hosted Unified Communications Services Customer Administration"	Describes the options available to Customer administrators within the Hosted Unified Communications Services (UCS) system.
Appendix D, "Sample PGW, Unified CM, and IP Unity Transactions"	Describes the sample PGW, Unified CM and IP Unity transactions in Unified UCS
Appendix E, "Local Gateway Supported Call Scenarios"	Describes the Local Gateway supported call scenarios in Cisco Hosted UCS
Appendix F, "Legacy PBX Information"	Describes the Leagacy PBX Information for the Hosted UCS Release 7.1(a)
Appendix G, "Phone Details"	Provides the details of Phone Types name and model ID list.
Appendix H, "Local Gateway Configuration"	Provides the Example Local Gateway Configuration.

Related Documentation

For more information, see the following guides:

- *Release Notes for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a),* http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/7.1a/release/hucrn71a.html
- *Software Support Matrix for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a)* http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/7.1a/softwarematrix/hucsmatrix71a.html
- *Getting Started with Cisco Hosted Unified Communications Services, Release 7.1(a)* http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/7.1a/user/getstart7.1a.html
- *Solutions Reference Network Design for Cisco Hosted Unified Communications Services (Hosted UCS), Release 7.1(a)*

  To obtain a copy of the Solution Reference Network Design document for Cisco Hosted Unified Communications Services, Release 7.1(a), contact your Cisco representative.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

Document Conventions

This document uses the following conventions:

<table>
<tr><th>Convention</th><th>Description</th></tr>
<tr><td>boldface font</td><td>Commands and keywords are in boldface.</td></tr>
<tr><td>italic font</td><td>Arguments for which you supply values are in italics.</td></tr>
<tr><td>[ ]</td><td>Elements in square brackets are optional.</td></tr>
<tr><td>{ x | y | z }</td><td>Alternative keywords are grouped in braces and separated by vertical bars.</td></tr>
<tr><td>[x | y | z]</td><td>Optional alternative keywords are grouped in brackets and separated by vertical bars.</td></tr>
<tr><td>string</td><td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td></tr>
<tr><td><code>screen</code> font</td><td>Terminal sessions and information the system displays are in <code>screen</code> font.</td></tr>
<tr><td><code>boldface screen</code> font</td><td>Information you must enter is in <code>boldface screen</code> font.</td></tr>
<tr><td>italic screen font</td><td>Arguments for which you supply values are in italic screen font.</td></tr>
<tr><td>^</td><td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td></tr>
<tr><td>< ></td><td>Nonprinting characters, such as passwords are in angle brackets.</td></tr>
</table>

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

CHAPTER 1

Hosted UCS Call Routing and Dial Plans

This chapter describes how call routing occurs and how dial plan models work within a Cisco Multi-tenant Hosted Unified Communications Services (UCS) 7.1(a) deployment. It also describes how to use the Vision OSS Unified Services Manager (USM) application to load dial plan models. This section includes the following sections:

Overview

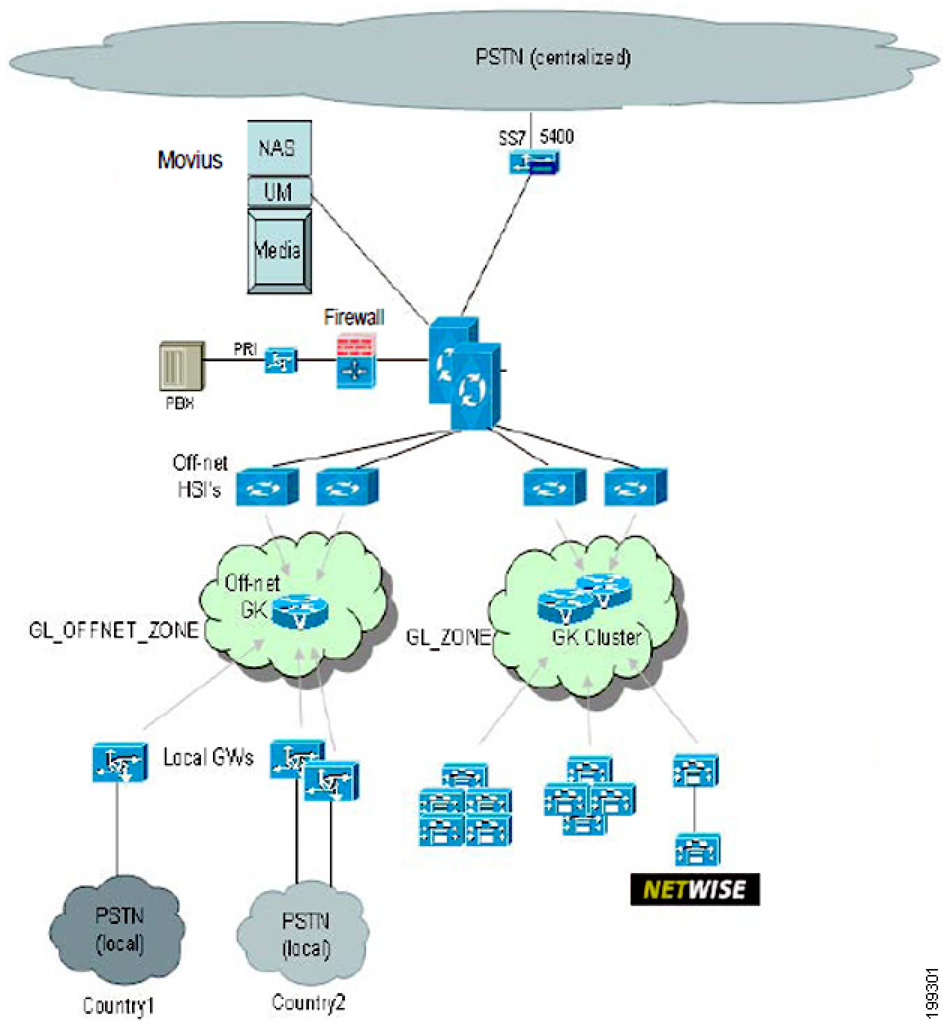
This section describes how call routing occurs in a Hosted UCS system and includes the following topics:

Hosted UCS System Overview

Hosted UCS is a distributed IP telephony system supporting one or more customers, at one or more locations for each customer. The telephony service is provided using primarily Cisco infrastructure, such as Cisco PGWs, Cisco Unified CMs and gatekeepers. The implementation may also include third-party products such as Movius (IP Unity) VoiceMail. USM is an integral part of the Hosted UCS system, provided by VisionOSS, a key Cisco partner involved in the development and deployment of Hosted UCS.

USM is a provisioning system that can be used to automate and standardize the configuration of the many network devices required for a large-scale, multi-tenant deployment of Cisco Unified CM.

Figure 1-1 Hosted UCS System



The Hosted UCS solution supports automatic provisioning of customer locations in different countries, with appropriately configured PSTN dialing rules.

The diagram in Figure 1-1 shows an overview of the solution components including IP Unity and Netwise. It also illustrates features including multiple PGWs, Legacy PBXes, local PSTN gateways and centralized gateways.

Numbering

To support multiple tenants on a common infrastructure with overlapping number capability, it is necessary to use longer internal numbers within the system, which include the following four sub-components:

- CPID (Call Processing ID): A unique system-wide ID for a Unified CM, Cisco PGW or IP Unity system, which is dynamically allocated by USM
- RID (Routing ID): A value for a Location, unique per CPID, which is dynamically allocated by USM

- SLC (Site Location Code): An admin-entered ID (unique within customer only) for a customer location. The user dials this number (for example, 711) for inter-site calls
- Extension: The local extension of an IP Phone (for example, 001)

For multi-tenant deployments, directory numbers on IP Phones are a concatenation of these four sub-components in the following order:

CPID + RID + SLC + EXTENSION

Dialing Conventions

Generally speaking, IP Phone users can make three types of calls:

- Intra-site calls: extensions at the same customer location by dialing just the EXTENSION they wish to reach
- Inter-site calls: extensions at other locations belonging to the same customers by dialing an inter-site prefix (typically 8) followed by SLC followed by EXTENSION
- PSTN calls: Destinations in the PSTN by dialing the PSTN breakout code (typically 9 or 0) followed by the E.164 number of the PSTN endpoint they wish to reach.

When the destination E.164 number corresponds to an IP Phone running within the Hosted UCS infrastructure, the system automatically routes the call to the identified endpoint. It presents the caller as an internal source if the caller belongs to the same customer as the called party. This type of call is known as a forced on-net call.

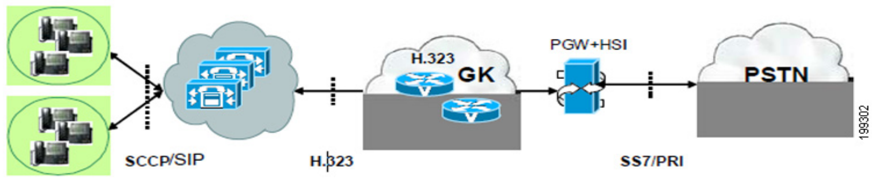
Call Routing Between Cisco PGW and Unified CM

This section describes how call routing occurs between the Cisco PGW and a Unified CM cluster. It includes the following topics:

Cisco PGW to Unified CM Interface

The demarcation point between Unified CM and the Cisco PGW/HSI is an H.323 trunk, which is provisioned as an H.225 gatekeeper-controlled trunk on Unified CM. This trunk can be viewed as an internal interface in the system architecture (see Figure 1-2).

Figure 1-2 H.323 Interface between the Cisco PGW and Unified CM



Calls may traverse this interface in either direction:

- From Unified CM to Cisco PGW
- From Cisco PGW to Unified CM

In either case, the gatekeeper routes the call.

When the call is sent from the Cisco PGW towards Unified CM, the Cisco PGW must ensure that the called number begins with the CPID of the Unified CM Cluster on which the endpoint resides. Each Unified CM cluster registers with the gatekeeper using its CPID as tech-prefix, which ensures that the call reaches the correct cluster.

When the Unified CM initiates a call towards the Cisco PGW it sets the called number based on rules that ensure that called numbers begin with the appropriate digit (for example, 8 for internal calls or 9 for PSTN calls). No Unified CM Cluster should be registered to the gatekeeper with a CPID beginning with 8 or 9, so the gatekeeper can use its *default technology prefix* (configured to 999#) to route this call. The HSI registers with the gatekeepers using this default technology prefix to receive these calls and deliver them to the Cisco PGW.

Unified CM to Cisco PGW Call Routing

Different types of calls are supported from Unified CM to Cisco PGW, and for each type, the Unified CM inserts a single Call Type (CT) digit into the calling number so that the Cisco PGW can detect the call type. The following call types may be sent from Unified CM to the Cisco PGW:

- Emergency calls (CT=4).
- Basic calls from an IP Phone at a customer location to another IP Phone at a location belonging to the same customer. (CT=8).
- Calls forwarded by an IP Phone at a customer location to another IP Phone at a location belonging to the same customer. (CT=6).
- Basic calls from IP Phones to the PSTN (CT=9)
- Calls forwarded by IP Phones to the PSTN (CT=5).
- Calls generated by certain applications (for example, Netwise) that need to reach endpoints that do not all belong to the same customer (CT=7).

For calls from Unified CM to the Cisco PGW, the Unified CM must always include the Call Type digit with the Calling Number in the following format:

Calling Number = CPID + RID + CT + SLC + EXTENSION.

If CT=9 or 5 (basic call to PSTN) then the Called Number must start with 9 followed by a normalized PSTN number beginning with either a 0 for a national PSTN call or 00 for an international call. For example, calls from a UK IP Phone to the PSTN would have the called number in the format 9+0+*nationalnumber* or 9+00+*internationalnumber*.

If CT=8 or 6 (inter-site calls) then the Called Number must equal 8 + SITECODE + EXTENSION. Unified CM normalizes the Inter-Site-Prefix to 8 as necessary for customers who have been provisioned to use another value when dialing between sites.

Cisco PGW to Unified CM Call Routing

The following types of call are sent from the Cisco PGW to Unified CM

- Calls from the PSTN
- Calls from other internal endpoints (e.g. IP Phones or PBX extensions).
- Calls to Unified CM resources such a Message Waiting Indicator On or Off devices.

In all these cases, the Cisco PGW sets the called party number (B number) to the full internal number of the phone (or MWI device) that it wishes to reach. In the typical case where the called endpoint is an IP Phone, the calling number (A number) is set by the Cisco PGW to indicate the caller. This allows the destination IP phone user to automatically redial the caller, using a directory of received or missed calls. In the case of calls to the MWI On or Off devices, the calling number is set to the full internal number of the IP Phone whose message waiting light must be set or cleared.

Example Calls

The following calls illustrate the format of calling and called numbers on call legs that cross the interface between Unified CM and the Cisco PGW.

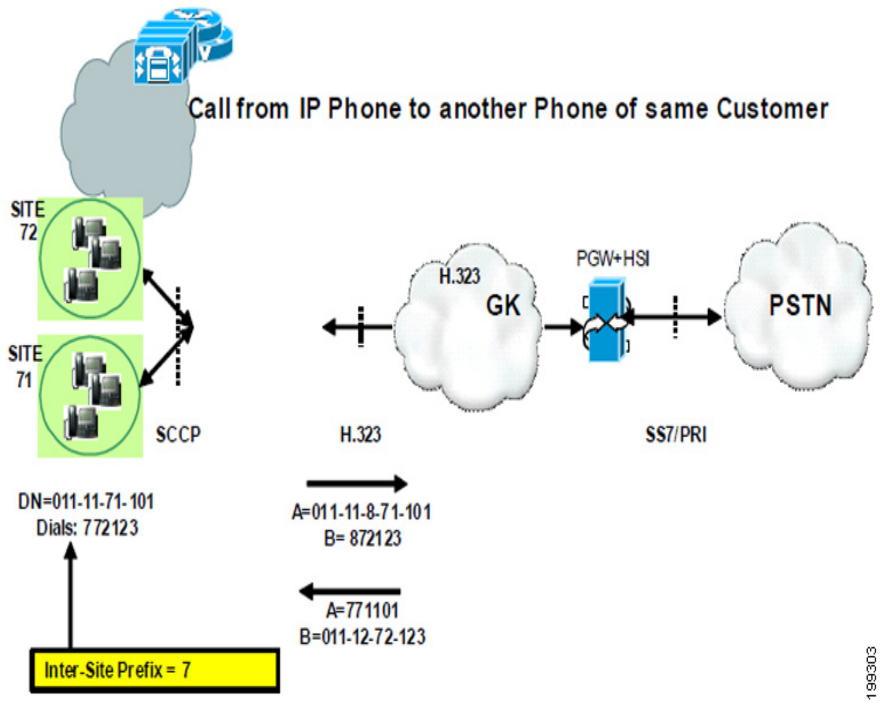
Inter-site call (Call Type = 8)

Figure 1-3 shows numbering on the Unified CM-to-Cisco PGW interface for the two call legs (from Unified CM to the Cisco PGW and back to Unified CM) associated with an inter-site call from a phone (Site 71) belonging to one customer and another phone at a different Site (Site 72) belonging to the same customer.

On the upward leg from Unified CM to the Cisco PGW, the calling number includes the CT=8 and the called number starts with an 8 regardless of the actual inter-site-prefix configured and dialed by the user.

On the downward call leg from the Cisco PGW to Unified CM, the called number is the Unified CM DN of the phone that will ring. The Unified CM DN is made up of the CPID + RID + SLC + EXTENSION and is known as the Full Internal Number (FINT). The calling number is formatted by the Cisco PGW into an internal number format that can be dialed by the called phone to reach the caller.

Figure 1-3 Numbering on H.323 Interface for Two Call Legs Associated with an Inter-site Call

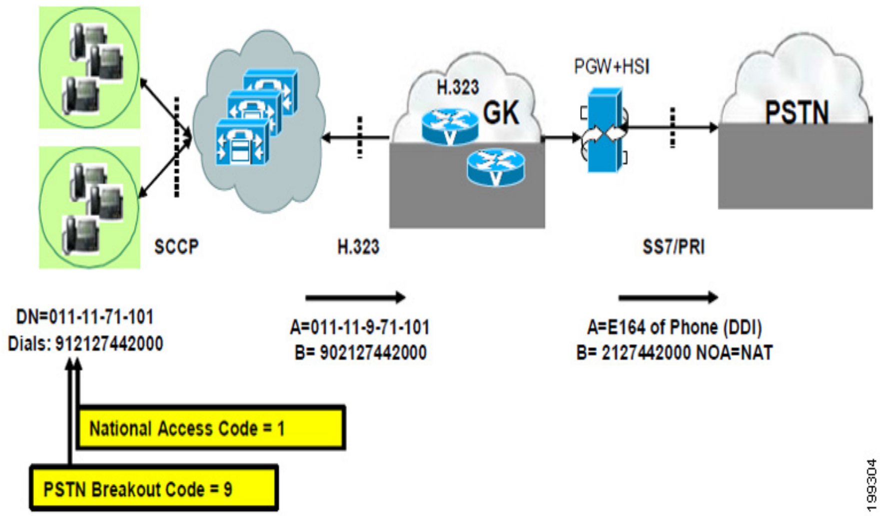


Call from IP Phone to National PSTN (Call Type = 9)

If CT=9 or 5 (basic call to PSTN) then the Called Number must equal 9 followed by a normalized PSTN number beginning with either a 0 for a national PSTN call or 00 for an international call. For example, calls from a UK IP Phone to the PSTN would have the B-number in the format 9+0+*nationalnumber* or 9+00+*internationalnumber*.

Figure 1-4 shows the numbering of called and calling part number on the interface between Unified CM and the Cisco PGW for a call from IP Phone at a US location to the national PSTN. Note that the US long distance trunk selection code (1) has been replaced by a 0 to normalize this call for processing by the Cisco PGW.

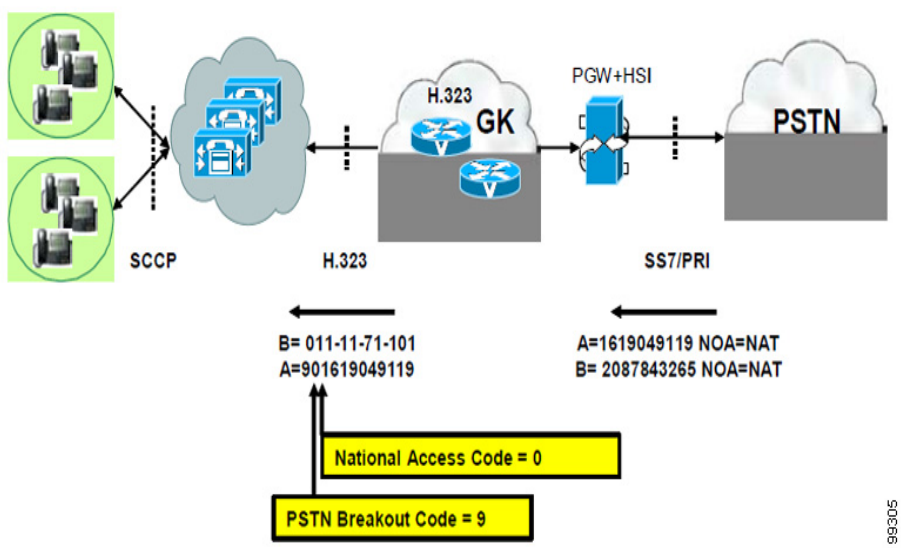
Figure 1-4 Numbering on interface between Unified CM and the Cisco PGW for a National PSTN Call in US



Call from PSTN to Unified CM

Figure 1-5 shows the numbering convention used on the interface between the Cisco PGW and Unified CM when sending calls toward an IP Phone. Note that no Call Type is used in the calling number in this direction. The called number corresponds directly to the Full Internal Number of the phone being called. The calling number has been formatted by the Cisco PGW so that the destination phone directory service can be used to redial the caller later. The calling number begins with the PSTN breakout code for the caller's location (country) (for example, 9 in the UK, followed by the national or international trunk access prefix for that country.

Figure 1-5 Inbound Call from PSTN to IP Phone



Gatekeeper Call Routing

This section describes how call routing occurs between a H.323 gatekeeper, a Cisco PGW, and the Unified CM cluster. It includes the following topics:

Cisco H.323 Gatekeepers

The Hosted UCS multi-tenant dialplan does not dynamically change the Cisco gatekeeper configuration. The gatekeeper configuration is manually setup at the start of deployment. The gatekeeper learns about H.323 devices, such as Unified CM trunks or IOS PSTN gateways, when USM provisions the systems to register with the gatekeepers. Gatekeepers route calls between:

- Cisco PGW and Cisco Unified CMs (mandatory)
- Cisco PGW and Local PSTN gateways (optional)

Cisco gatekeepers must be used because call routing uses the Cisco-proprietary *technology prefix* for routing calls. The Hosed UCS platform has been tested using gatekeeper clustering for high availability, using the GUP protocol.

Routing calls between the Cisco PGW and Unified CM and local PSTN gateways is logically distinct but gatekeeper device or cluster may provide both roles.

Gatekeeper Routing between Cisco PGW and Cisco Unified CM

An H.323 zone HUCS_ZONE is used for routing calls between the Cisco PGW and Unified CM. A pool of Cisco HSI dedicated to Cisco PGW-to-Unified CM calls and the Unified CM clusters register within this zone. The Cisco PGW uses the *Unified CM* dialplan for handling calls received from these HSI and a dedicated route list (*rltist2hsi)* to send calls through the HSI to the Unified CM Clusters.

Call routing within this zone is based entirely on the technology prefix, which as explained earlier form the leading digits of the called number. There is no inter-zone call routing used in this solution.

The Cisco Unified CM clusters will be automatically configured by USM to register with the gatekeeper zone HUCS_ZONE using the CPID as the technology prefix. Because the Cisco PGW always sends calls to a Unified CM via the gatekeeper with a called number beginning with the CPID of a Unified CM cluster calls are routed to the correct cluster. The gatekeeper simply analyses the called number that matches its leading digits to the CPID of registered Unified CM clusters.

The HSI must register with a technology prefix of 999#, which must also be configured as the default technology prefix. This means that a call that does not start with a valid CPID is automatically be sent to the HSI for handling by the Cisco PGW. Unified CM Clusters must never use a CPID of 999#.

Using Dial Plan Models

This section describes how dial plan models control call routing within the Hosted UCS system. It includes the following topics:

- Associating the Dial Plan with the Cisco PGW, page 1-13
- Edit Dial Plan and association, page 1-13

The Hosted UCS dial plan is a set of rules for provisioning multiple products in a coordinated way to achieve a coherent and distributed call routing framework. The intent is to provide a multi-tenant architecture where the infrastructure is shared by one or more customers. It includes rules for provisioning four products:

- Cisco PGW
- Cisco Unified CM
- Cisco IOS gateways
- IP Unity

Only the first three components are used for call routing.

The purpose of using models (loaders) is to add configuration into the USM database. Models are created using Microsoft Excel files and USM loads the configuration by importing the Excel files. Importing these spreadsheets updates the USM database but does not actually provision the components. The data in the models is in the form of templates that are used by USM to provision the network components through a later operation.

There are currently five supported dial plan models, each in a separate Excel worksheet within a single Excel file. Sheets can be in different Excel files but it is common practice to keep all models in the same file. Each sheet is imported into USM using different USM bulk load tools.

Model data can be used multiple times by USM to provision network components. Variables within each (delimited by #) are substituted with specific values by USM for individual transactions.

Accessing USM and Initial Setup

This section describes the steps required to access USM and perform the initial setup. It includes the following sections:

- Accessing the USM GUI, page 1-9
- Creating an Internal System Superuser, page 1-10
- Defining Basic Setup Components, page 1-10
- Adding additional Phone Types (optional), page 1-11

Accessing the USM GUI

To access the USM GUI, perform the following steps:

Procedure

Step 1 Use the appropriate IP address to access the relevant USM server:

Step 2 Log in as the superuser:

- Username—**bvsm**
- Password—**password**

When logging in for the first time, you are prompted to change the password for USM.

Step 3 Change the password of the superuser **bvsm** to an appropriate strong password, for example **ipcbuemea**.

Creating an Internal System Superuser

To create an internal system superuser, perform the following steps:

Procedure

Step 1 Choose **General Administration > Users**.

Step 2 Click **Add**.

Step 3 Add the following:

- Username—<*username*>
- Password—<*password*>
- Role—**Internal System SuperUser**
- First name—<*name*>
- Last name—<name>

Step 4 Click **Next >>**.

Step 5 Choose the following:

- Web presentation theme—**Default GUI Branding**
- Preferred country—<*country*>
- Access profile—Default

Step 6 Click **Add**.

Step 7 Log out of USM and log in with the new username.

When logging in for the first time, you are prompted to change the password.

Defining Basic Setup Components

To prepare USM by loading the base system data (1-BaseData worksheet), perform the following steps:

Procedure

Step 1 Choose **Setup Tools > Bulk load Samples**.

Step 2 Click **01 - Base System Data**.

Step 3 Click **Save** to save in your local mahcine.

Step 4 Browse **General Tools > Bulk Load.**

Step 5 Schedule a new job to upload **1-BaseData sheet.**

Step 6 Click **Submit.**

This loads the information from the BaseData worksheet into the USM database, including the following:

- Default Cisco Unified CM phone button templates

- Valid Cisco Unified CM phone types and expansion module
- Service types, which are used in the Cisco Unified CM model for defining class of service (CoS) configuration. This is customer-specific.
- Dial plans and Hardware sets
- Associate Hardware sets with the dial plan
- Add countries

Note Check for any errors or warnings at the completion of loading.

Adding additional Phone Types (optional)

Note If the uploaded Base System Data does not have the required Phone type then you can manually add a phone type into USM for provisioning. Follow the steps below to add a phone type,

Step 1 Navigate to **Setup Tools > Phone Types >Phone Type Management.**

Step 2 Click Add to add a new phone type

Step 3 Under **Details**, enter the following:-

- Name—<PhoneTypeName>, for example **7925 SCCP**
- Product—<ProductName>, for example **Cisco 7925**
- Product Model ID—<ProdModID>, for example **484**
- Protocol—<PhoneProtocol>, for example **SCCP**

Step 4 Select other details according to phone model support

Step 5 Click **Add.**

Note Product Model ID value is a unique number for each phone model which should match with CUCM supported phone model IDs.

Note If the phone type is added after provisioning dial plan, hardware sets and providers on USM, the associated dial plan with hardware set needs to be disconnected and connected back again so that the new phone type is available under the provider.

This section explains how to define the dial plan type in USM, associate the dial plan to the hardware set that defines which components can be used in the deployment and edit the dial plan and association.

This section includes the following topics:

- Defining the Dial Plan Type, page 1-12
- Associating the Dial Plan with the Cisco PGW, page 1-13

- Edit Dial Plan and association, page 1-13

Defining the Dial Plan Type

When a dial plan is created, parameters are configured that define how the Hosted UCS environment is provisioned.

Caution You should use the default dial plan models; Do not create a new dial plan or modify an existing dial plan without assistance from Cisco Advanced Services (AS) or VisionOSS.

To define the dial plan type, complete the following steps:

Procedure

Step 1 Choose **Dialplan Tools > Number Construction**.

Step 2 Click **Add**.

Step 3 From the Details menu, complete the following fields, as shown in this example:

- Name—**HUCS**
- Description—**Hosted UCS 7.1a Dial Plan**

Step 4 From the Codec Selection menu, complete the following fields:

- Intra-region Codec—<*intra_region_codec*>
- Inter-region Codec—<*inter_region_codec*>

Step 5 From the Single/Multi-Tenant Capable menu, click **Multi-Tenant Dial Plan**.

Step 6 From the Internal Number Format menu, do the following:

a. Click **Includes CPID**.
b. Enter CPID Digits—<*CPID*>; for example, **3**.
c. Click **Includes RID**.
d. Enter RID Digits—<*RID*>; for example, **4**.
e. Click **Includes Site Code**.
f. Enter Max. Site Code Digits—<*MaxSiteCodeDigitLength*>; for example, **3**.
g. Enter Site Code Rules—<*SiteCodeRules*>; for example, **3**.
h. Click **Variable Length Internal Number**.

Step 7 From the RID Type Selection menu, add the Routing Identifier (RID)—**Location RID**.

Step 8 From the Dial Prefixes menu, do the following:

- Click **Inter-Site Prefix Required**.
- Click **Inter-Site Prefix Configurable**.
- Click **PSTN Access Prefix Required**.
- Click **PSTN Access Prefix Configurable**.

Step 9 From the Format of External Phone Number Mask menu, do the following:

- Select the format of the External Phone Number Mask on Unified CM Device Line Configuration page.

Step 10 Click **Add**.

Associating the Dial Plan with the Cisco PGW

After the dial plan is created, it must be connected with the Cisco PGW-CCM hardware set that identifies the network components associated with the dial plan.

To connect the dial plan, perform the following steps:

Procedure

Step 1 Choose **Dialplan Tools > Hardware Sets**.

Step 2 Click **Associated DialPlans** next to the PGW-CCM hardware set.

Step 3 Click **Connect** to connect the desired dial plan.

Edit Dial Plan and association

This section describes required steps to edit the dial plan in USM. Following topics are included :

- Edit Dial Plan, page 1-13
- Connect Dial Plan with Hosted Unifed Communication Services Hardware Set, page 1-14

Edit Dial Plan

When a dial plan is created, a number of parameters are configured which defines how the Hosted UCS environment is provisioned. To edit an already created dial plan:

Step 1 Choose **Dialplan Tools > Number Construction**.

Step 2 Click **HUCS Dial Plan.**

Step 3 Under **Details**, use the following settings:

- Name—**HUCS**
- Description—**HUCS Dial Plan**

Step 4 Under **Codec Selection**, add the following:

- Intra-region Codec: <intra_region_codec> (for Hosted UCS 7.1(a) choose **G.711**)
- Inter-region Codec: <inter_region_codec> (for Hosted UCS 7.1(a) choose **G.711**)

Step 5 Under **Dial Plan Rules,** do the following:

- Check the **Multi-Tenant Dial Plan?** check box
- Check the **Enforce HUCS Dial Plan?** check box

- Under **Internal Number Format**, ensure the following:
- Check the **Includes CPID?** check box
- CPID Digits—<CPID>, for example **2**
- Check the **Includes RID?** check box
- RID Digits—<RID>, for example **4**
- Check the **Includes Site Code?** check box.
- Max. Site Code Digits—<MaxSiteCodeDigitLenght>, for example **3**
- Site Code Rules—<SiteCodeRules>, for example **3**
- Check the **Variable Length Internal Number?** check box
- Under **RID Type Selection**, enter the following:
- Routing Identifier (RID)—**Location RID**

Step 6 Under **Dial Prefixes**, do the following:
- Check the **Inter-Site Prefix Required?** check box.
- Check the **Inter-Site Prefix Configurable?** check box
- Check the **PSTN Access Prefix Required?** check box
- Check the **PSTN Access Prefix Configurable?** check box

Step 7 Under **Format of External Phone Number Mask** on Unified CM, do the following:
- Select the format of the External Phone Number Mask on Unified CM Device Line Configuration page. For Hosted UCS 7.1(a) testing select **Show National Code Prefix** and **Show National Code.**

Step 8 Under **Format of IPPBX Configured Internal Number**, do the following:
- Uncheck the **Includes CPID** check box
- Uncheck **Includes RID** check box
- Ensure **Includes SiteCode** is selected
- Ensure **Includes Extension** is selected

Step 9 Click **Modify.**

Connect Dial Plan with Hosted Unifed Communication Services Hardware Set

Note This step is to be done if the hardware set is not already associated with Hosted UCS dial plan

To connect the dial plan, do the following:

Step 1 Choose **Dialplan Tools > Hardware Sets.**

Step 2 Click **Associated DialPlans** corresponding to the HUCS hardware set.

Step 3 Click **Connect** in order to connect the desired dial plan.

Loading the Dial Plan Models

This section describes the steps for loading the core Hosted UCS 7.1(a) models (Cisco PGW and Cisco Unified CM). The models define how USM should configure the Cisco PGW and Cisco Unified CM. This section includes the following topics:

- Loading the Cisco Unified CM Model, page 1-15
- Loading the PGW MML Model, page 1-15
- Loading the PGW TimesTen Model, page 1-15

Loading the Cisco Unified CM Model

To prepare USM by loading the Cisco Unified CM model, perform the following steps:

Procedure

Step 1 Choose **Dialplan Tools > Configuration Models**.

Step 2 Click **Schedule new job**.

Step 3 Browse for the CCM model and click **Submit**.

Note Check for any errors or warnings at the completion of loading.

Loading the PGW MML Model

To prepare USM by loading the PGW model, perform the following steps:

Procedure

Step 1 Choose **Dialplan Tools > Configuration Models**.

Step 2 Click **Schedule new Job**.

Step 3 Browse for the PGW MML model and click **Submit**.

Note Check for any errors or warnings at the completion of loading.

Loading the PGW TimesTen Model

To prepare USM by loading the PGW TimesTen Model, perform the following steps:

Step 1 Choose **Dialplan Tools > Configuration Models**.

Step 2 Click **Schedule New Job**.

Step 3 Browse for the PGW-Times-Ten model and click **Submit**.

Note Note: Check for any errors or warnings at the completion of loading.

CHAPTER 2

Hosted UCS Static Configuration

This chapter describes the static configuration required as part of the lab builds for Cisco Hosted Unified Communications Services (UCS), Release 7.1(a).

This chapter includes the following sections:

- Cisco Unified Communication Manager Static Configuration, page 2-1
- Cisco PGW Static Configuration, page 2-8
- Cisco HSI Static Configuration, page 2-26
- Cisco Gatekeeper Static Configuration, page 2-27

Cisco Unified Communication Manager Static Configuration

This section details the static (manual) configuration required for certain Unified CM configuration parameters which cannot be provisioned through AXL SOAP. The following settings need to be configured manually on the Unified CM:

- Server Configuration, page 2-1
- Date/Time Configuration, page 2-2
- Enterprise parameters Configuration, page 2-2
- Automated Alternate Routing Group Configuration, page 2-3
- Conference Bridge Configuration, page 2-3
- Transcoder Configuration, page 2-4
- Cisco Unified IP Phone Services Configuration, page 2-4
- Phone Button Template Configuration, page 2-7
- Softkey Template Configuration, page 2-7

Server Configuration

Use the server configuration to specify the IP address of the server where the Cisco Unified Communications Manager is installed.

Procedure:

Step 1 Choose **System > Server.**

Step 2 Enter the following:

- Host Name/IP Address—Full IP address of the server, for example **10.131.2.2**
- Description—Description of the server, for example **e2c1p**

Date/Time Configuration

Date/Time Groups are used to define time zones for the various devices that are connected to Cisco Unified Communications Manager. Each device exists as a member of only one device pool, and each device pool has only one assigned Date/Time Group. USM uses the international standard zoneinfo database, also called the tz database. In USM, the timezone names are all in the form Area/Location, where Area is the name of a continent or ocean, and Location is the name of a specific location within that region, usually cities or small islands, such as "America/New_York".

Procedure:

Step 1 Choose **System > Date/Time Group.**

Step 2 Perform the following settings:

- Group Name—for example **Europe-London**
- Time Zone—Choose the time zone from the drop-down list box, for example: **(GMT) Etc/GMT0**
- Separator—Choose the separator character to use between the date fields, for example **/**
- Date Format—Choose the date format for the date that displays on Cisco Unified IP Phones, for example: D/M/Y
- Time Format—Choose a 12-hour or 24-hour time format, for example **24-hour**

Note Group name format in USM is "Area/Location", and in Unified CM is "Area-Location".

Enterprise parameters Configuration

Enterprise parameters provide default settings that apply to all devices and services in the same cluster.

Procedure:

Step 1 Choose **System > Enterprise Parameters**.

Step 2 In the **Enterprise Parameters Configuration section** change **Advertise G722 Codec—Disabled**

Step 3 In the **Phone URL Parameters section** change **URL Directories**—http://<virtual_IP_address_of_USM_server>/bvsmweb/directoryservices.cgi, for example **http://10.100.92.33/bvsmweb/directoryservices.cgi**

Note This parameter specifies the URL that Cisco Unified IP Phone models use when the Directory button is pressed. This should point to the virtual IP address of the USM server (not Unified CM server):

Step 4 If your network does not use DNS services, replace the Unified CM Publisher Server name with the IP address of the Unified CM Publisher Server in the following fields in the Phone URL Parameters section:

- URL Authentication—Enter http://<IP_address_of_Publisher_server>:8080/ccmcip/authenticate.jsp, for example **http://10.132.4.2:8080/ccmcip/authenticate.jsp**
- URL Information—Enter http://<IP_address_of_Publisher_server>:8080/ccmcip/GetTelecasterHelpText.jsp, for example **http://10.132.4.2:8080/ccmcip/GetTelecasterHelpText.js**p
- URL Services fields—Enter http://<IP_address_of_Publisher_server>:8080/ccmcip/getservicesmenu.jsp, for example **http://10.132.4.2:8080/ccmcip/getservicesmenu.jsp**

Automated Alternate Routing Group Configuration

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number when Unified CM blocks a call due to insufficient location bandwidth.

Note This only applies to Unified CM 7.x and Unified CM 6.x.

Procedure:

Step 1 Choose **Call Routing > AAR Group.**

Step 2 Enter the following:

- AAR Group Name—for example, **defaultaar**
- Prefix Digits—Leave this blank

Conference Bridge Configuration

Note This is an optional step, and is only required if Conference Bridges are deployed in the network.

The Conference Bridge for Cisco Unified Communications Manager is either a software or hardware application. It allows both ad hoc and meet-me voice conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

For further details on how to configure a Conference Bridge, refer to:

- For Unified CM 6.1(x)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_1_1/ccmcfg/b04cnbrg.html
- For Unified CM 7.1(x)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b04cnbrg.html

Transcoder Configuration

Note This is an optional step, and is only required if Transcoders are deployed in the network.

The Media Resource Manager (MRM) has responsibility for resource registration and resource reservation of transcoder within a Cisco Unified Communications Manager (CUCM) cluster. Cisco Unified Communications Manager simultaneously supports registration of both the Media Termination Point (MTP) and Transcoder and concurrent MTP and transcoder functionality within a single call.

The CUCM invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two disparate codecs to enable communications between them.

For further details on how to configure a Transcoder, refer to:

- For Unified CM 6.1(x)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_1_1/ccmcfg/b04trans.html
- For Unified CM 7.1(x)
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b04trans.html

Cisco Unified IP Phone Services Configuration

Users can subscribe to the Cisco Unified IP Phone Services created by the Administrators. Depending on the deployment, the following services should be created:

- Login/Logout Services for extension mobility, page 2-4
- Roaming Login/Logout Services for USM user roaming, page 2-5
- Cisco Unified IP Phone XML Services, page 2-6

Note Login/Logout Services for extension mobility are used only if one customer is to be provisioned per cluster . If this is not the case then only Roaming Login/Logout Services for USM user roaming can be used.

Login/Logout Services for extension mobility

To enable Login/Logout Services for extension mobility for Unified CM 4.2(3) do the following:

Step 1 Choose **Feature > Cisco Unified IP Phone Services**.

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Login/Logou**t
- Service Description—**Extension Mobility Service**
- Service URL—Enter http://<Publisher_IP_Address>/emapp/EMAppServlet?device=#DEVICENAME#, for example: **http://10.131.4.2/emapp/EMAppServlet?device=#DEVICENAME#**

Step 3 Check the **Enable** check box.

To enable Login/Logout Services for extension mobility for Unified CM 7.1(3) and 6.1 (4) do the following:

Step 1 Choose **Device > Device Settings > Phone Services**.

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Login/Logout**
- Service Name (ASCII Format)—**Login/Logout**
- Service Description—**Extension Mobility Service**
- Service URL—Enter http://<Publisher_IP_Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#, for example: **http://10.132.4.2:8080/emapp/EMAppServlet?device=#DEVICENAME#**

Step 3 Check the **Enable** check box.

Roaming Login/Logout Services for USM user roaming

To enable Roaming Login/Logout Services for USM user roaming for Unified CM 4.2(3) do the following:

Step 1 Choose **Feature > Cisco Unified IP Phone Services.**

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Roaming Login/Logout**
- Service Description—**Extension Mobility Service**
- Service URL—Enter http://<USM_Virtual_IP_Address>/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME, for example: **http://10.100.92.33/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME#**

Step 3 Check the **Enable** check box.

To enable Roaming Login/Logout Services for USM user roaming for Unified CM 6.1 (x) and 7.1 (x) do the following:

Step 1 Choose **Device > Device Settings > Phone Services.**

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Roaming Login/Logout**
- Service Name (ASCII Format)—**Roaming Login/Logout**
- Service Description—**Extension Mobility Service**
- Service URL—Enter http://<USM_Virtual_IP_Address>/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME, for example: **http://10.100.92.33/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME#**

Step 3 Check the **Enable** check box.

Cisco Unified IP Phone XML Services

To enable Cisco Unified IP Phone XML Services for Unified CM 4.2(3) do the following:

Step 1 Choose **Feature > Cisco Unified IP Phone Services.**

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Phone Services**
- Service Description—**Phone Services**
- Service URL—Enter http://<USM_Virtual_IP_Address>/bvsmweb/bvsmservices.cgi?device=#DEVICENAME, for example: **http://10.100.92.33/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#**

To enable Cisco Unified IP Phone XML Services for Unified CM 6.1 (x) and 7.1(x) do the following:

Step 1 Choose **Feature > Cisco Unified IP Phone Services.**

Step 2 Add the **Cisco Unified IP Phone Service** using the following settings:

- Service Name—**Phone Services**
- Service Name (ASCII Format)—**Phone Services**
- Service Description—**Phone Services**
- Service URL—Enter http://<USM_Virtual_IP_Address>/bvsmweb/bvsmservices.cgi?device=#DEVICENAME, for example: **http://10.100.92.33/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#**

Phone Button Template Configuration

Cisco Unified CM includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones. A number of default phone button templates are loaded into USM during initial setup.

If customers want to use any non-standard phone button templates, they need to define them in USM, and also need to add them manually into Unified CM.

To add non-standard phone button templates do the following:

Step 1 Choose **Device > Device Settings > Phone Button Template.**

Step 2 Select the required **Phone Button Template**, for example **Standard 7960**

Step 3 Use the following setting:

- Button Template Name—<unique_button_template_name>, for example **Standard 7960-2lines** and configure the required number of buttons:
- Feature—Choose the function of the phone button that you want to specify in the template, for example **Line**
- Label—Enter a description of the button, for example **Line 1**

Note Ensure that the required number of lines is set up on the template settings. Ensure that each phone button template is cloned from the standard phone type for each variant; for example, confirm that the Standard 7960-2line is based on the standard 7960 template and set the number of lines to 2.

Note The USM InitPBX Load fails if Phone Button Templates exists as a USM Service Setting instead of Cisco Unified CM. If a validation failure occurs, either add the missing phone button template into the Cisco Unified CM or delete unwanted phone button templates from USM. Phone button templates cannot be deleted from the USM database without first disconnecting the dial plans from the hardware sets (under Dial Plan Tools > Hardware Sets > Associated Dial plans). Remember to reconnect the required dial plans afterwards.

Softkey Template Configuration

Softkey template configuration allows the administrator to manage softkeys that the Cisco Unified IP Phones (such as model 7960) support. To add Softkey templates to Unified CM clusters do the following:

Step 1 Choose **Device > Device Settings > Softkey Template.**

Step 2 Use the following settings:

- Create a softkey template based on—<available_softkey_template>, for example **Standard User**
- Softkey Template Name—<unique_softkey_template_name>, for example **Softkey_Advanced**

These softkey templates can later be imported into USM for each Unified CM cluster, and assigned to a phone when the phone is registered via USM.

Note Once the new softkey template has been created, you can add additional application softkeys, and configure softkey positions. For detailed instructions refer to the relevant Cisco Unified CM Administration Guides.

Cisco PGW Static Configuration

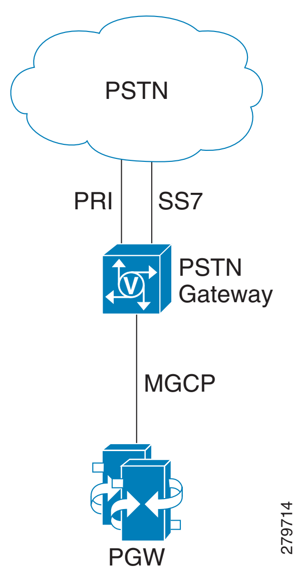
This section describes the required setup on the Cisco PGW before loading the USM platform. This section includes the following topics:

- Central Gateway PGW Breakout Configuration, page 2-8
- PGW/HSI/Unified CM Interface Configuration, page 2-9
- ILGW Dial Plan, page 2-11
- Example Cisco PGW Static Configuration, page 2-11
- PGW/HSI/Unified CM Interface Configuration, page 2-9
- Full Number Translation with TimesTen Database, page 2-17

Central Gateway PGW Breakout Configuration

One of the main features of the PGW in Hosted UCS 7.1(a) is to route calls to/from the PSTN. The "Central Gateway PGW" PSTN breakout can be achieved using the SS7 or PRI (MGCP controlled) signaling, as shown in Figure 2-1

Figure 2-1 Central Gateway PGW PSTN breakout



Depending on the deployment, a number of settings needs to be provisioned on the PGW, for example: External Nodes, Session Sets, MGCP Paths, IPFAS Paths, D-Channels, IP Links, DPCs, OPCs, APCs, Linksets, SS7 Routes, SS7 Paths and IP Routes.

For detailed information, refer to the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide.

Depending on the number of supported countries, a route list is to be provisioned on the PGW. To add a route list to PSTN for each country, for example U.K., do the following:

```
prov-add:rtlist:name="rtlist2pstn<Country_code>",rtname="route2pstn",distrib="OFF"
```

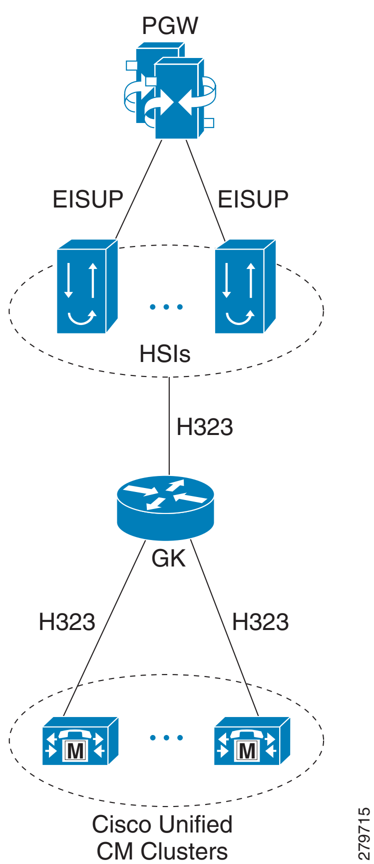
For example:

```
prov-add:rtlist:name="rtlist2pstn44",rtname="route2pstn",distrib="OFF"
```

PGW/HSI/Unified CM Interface Configuration

In Hosted UCS 7.1(a), the interface between the PGW/HSI and Unified CM clusters is an H.323 trunk (provisioned as a 'H.225 Gatekeeper controlled trunk' on Unified CM). The interface between the PGW and HSI is EISUP trunk, as shown in Figure 2-2

Figure 2-2 PGW/HSI/Unified CM Interfaces



Depending on the deployment and the number of HSIs needed, for the interface between the PGW and HSIs, a number of settings need to be provisioned on the PGW, for example:

```
prov-add:EXTNODE:NAME="hsi-ent4a",DESC="hsi-ent4a",TYPE="H323",ISDNSIGTYPE="N/A",GROUP=0
```

```
prov-add:EISUPPATH:NAME="eisup-hsi-ent4a",DESC="eisup-hsi-ent4a",EXTNODE="hsi-ent2a",MDO="
EISUP",CUSTGRPID="ICCM",ORIGLABEL="",TERMLABEL=""
prov-add:iproute:name="iproute-1",desc="IPRoute to 10.120.4.0 network",dest="10.120.4.0",
netmask="255.255.255.0", nexthop="IP_NextHop1", ipaddr="IP_Addr1",pri=1
prov-add:iproute:name="iproute-2",desc="IPRoute to 10.121.4.0 network",dest="10.121.4.0",
netmask="255.255.255.0", nexthop="IP_NextHop2", ipaddr="IP_Addr2",pri=1
prov-add:IPLNK:NAME="hsi-ent4a-iplnk-1",DESC="hsi-ent4a_IP_link_1",SVC="eisup-hsi-ent2a",I
PADDR="IP_Addr1",PORT=8003,PEERADDR="10.120.2.31",PEERPORT=8003,PRI=1,IPROUTE="iproute-1"
prov-add:IPLNK:NAME="hsi-ent4a-iplnk-2",DESC="hsi-ent4a_IP_link_2",SVC="eisup-hsi-ent2a",I
PADDR="IP_Addr2",PORT=8003,PEERADDR="10.121.2.31",PEERPORT=8003,PRI=2,IPROUTE="iproute-2"
```

For detailed information, refer to the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide.

The following needs to be provisioned on the PGW for PGW/HSI/Unified CM Interface Configuration:

- ICCM dial plan - ICCM is the dial plan which needs to be attached to the HSI trunk groups. This dial plan will be accessed when calls are passed from the HSIs to the PGW. To add the ICCM dial plan do the following:

```
numan-add:dialplan:custgrpid="ICCM", OVERDEC="YES"
```

- Trunk Group for each HSI. To add a trunk group do the following:

```
prov-add:trnkgrp:name="<trnkgrp_name>",clli="<clli_name>",svc="<signaling_svc>",type="
<type>",qable="<qable>",
```

for example:

```
prov-add:trnkgrp:name="1001",clli="hsi", svc=" eisup-hsi-ent4a",type="IP", qable="n"
```

- Routing Trunk Group for each HSI. To add the routing trunk group do the following:

```
prov-add:rttrnkgrp:name="<rttrnkgrp_name>",type=4,reattempts=0,queuing=0,cutthrough=3,
resincperc=0,
```

for example:

```
prov-add:
rttrnkgrp:name="1001",type=4,reattempts=0,queuing=0,cutthrough=3,resincperc=0
```

- Route to the HSI. To add the route trunk do the following:

```
prov-add:rttrnk:weightedTG="OFF",name="route2hsi",trnkgrpnum=<rttrnkgrp_name>,
```

for example:

```
prov-add: rttrnk:weightedTG="OFF",name="route2hsi",trnkgrpnum=1001
```

- To associate routing trunk groups for the remaining HSIs to the "route2hsi" route, add the following for each remaining HSI:

```
prov-ed:rttrnk:name="route2hsi",trnkgrpnum=<rttrnkgrp_name>,
```

for example:

```
prov-ed:rttrnk:name="route2hsi",trnkgrpnum=1002
```

- Route List to the HSI. To add the route list do the following:

```
prov-add:rtlist:name="rtlist2hsi",rtname="route2hsi",distrib="OFF"
```

- A minimum following HSI Trunk Group Properties should be provisioned: "CustGrpId", "AllowH323Hairpin" and "GatewayRBToneSupport". From HUCS 7.1(a) onwards, the trunk group properties should be added on a profile and the profile should be attached with trunk group for PGW 9.8(1). Follow the steps below if the profile is not available on PGW:

```
prov-add: profile:
name="<profile_name>",type="EISUPPROFILE",custgrpid="<custgrpid>",allowh323hairpin =
"1",gatewayrbtonesupport="1"
prov-add: trnkgrpprof:name="<trnkgrp_name>",profile="<profile_name>",
```

for example:

```
prov-add: profile:name="lvl1eisupf-1001",type="EISUPPROFILE",custgrpid="ICCM",
allowh323hairpin="1",gatewayrbtonesupport="1"
prov-add:trnkgrpprof:name="1001",profile=" lvl1eisupf-1001"
```

ILGW Dial Plan

The ILGW Dial Plan is used to route calls from Local Gateways. Because this dial plan is provisioned every time a country is added via USM, it need to be manually created. To add the ILGW dial plan:

```
numan-add:dialplan:custgrpid="ILGW", OVERDEC="Yes"
```

Example Cisco PGW Static Configuration

For the network shown in Figure 2-3, a sample Cisco PGW static configuration has been exported for the following files:

Config.mml

Routing.mml

ICCM.mml

ILGW.mml

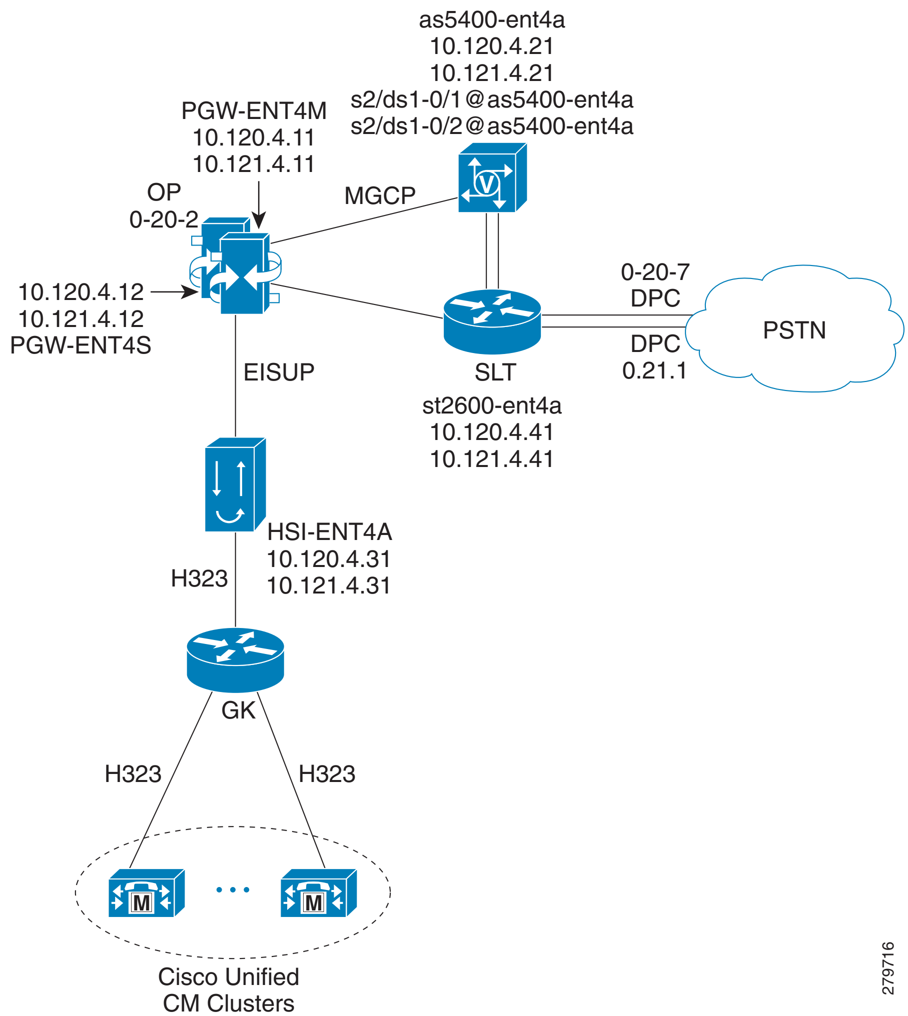
Properties.dat

Export_trkgrp.dat

Export_trunk.dat

XECfgParm.dat

Figure 2-3 Sample Network



Config.mml

```
prov-add:IPROUTE:NAME="iproute-2",DESC="IPRoute",DEST="10.121.2.0",NETMASK="255.255.255.0"
,NEXTHOP="IP_NextHop2",IPADDR="IP_Addr2",PRI=1
prov-add:IPROUTE:NAME="iproute-1",DESC="IPRoute",DEST="10.120.2.0",NETMASK="255.255.255.0"
,NEXTHOP="IP_NextHop1",IPADDR="IP_Addr1",PRI=1
prov-add:OPC:NAME="opc",DESC="opc",NETADDR="0.20.1",NETIND=2,TYPE="TRUEOPC"
prov-add:DPC:NAME="pstn1",DESC="pstn1 dpc",NETADDR="0.20.7",NETIND=2
prov-add:DPC:NAME="pstn2",DESC="pstn2 dpc",NETADDR="0.21.1",NETIND=2
prov-add:SS7PATH:NAME="ss7p-pstn1",DESC="SS7 path to
pstn1",MDO="ISUPV3_UK",CUSTGRPID="0000",SIDE="network",DPC="pstn1",OPC="opc",M3UAKEY="",O
RIGLABEL="",TERMLABEL=""
prov-add:EXTNODE:NAME="hsi-ent2a",DESC="hsi-ent2a",TYPE="H323",ISDNSIGTYPE="N/A",GROUP=0
prov-add:EXTNODE:NAME="slt2600-ent2a",DESC="slt2600-ent2a",TYPE="SLT",ISDNSIGTYPE="N/A",GR
OUP=0
prov-add:EXTNODE:NAME="slt2600-ent2b",DESC="slt2600-ent2b",TYPE="SLT",ISDNSIGTYPE="N/A",GR
OUP=0
prov-add:EXTNODE:NAME="as5400-ent2a",DESC="as5400-ent2a",TYPE="AS5400",ISDNSIGTYPE="N/A",G
ROUP=0
```

```
prov-add:EXTNODE:NAME="as5400-ent2b",DESC="as5400-ent2b",TYPE="AS5400",ISDNSIGTYPE="N/A",G
ROUP=0
prov-add:SESSIONSET:NAME="sset-slt-ent2a",EXTNODE="slt2600-ent2a",IPADDR1="IP_Addr1",PEERA
DDR1="10.120.2.41",PORT=7001,PEERPORT=7001,TYPE="BSM
V0",IPROUTE1="iproute-1",IPROUTE2="iproute-2",IPADDR2="IP_Addr2",PEERADDR2="10.121.2.41"
prov-add:SESSIONSET:NAME="sset-slt-ent2b",EXTNODE="slt2600-ent2b",IPADDR1="IP_Addr1",PEERA
DDR1="10.120.2.42",PORT=7001,PEERPORT=7001,TYPE="BSM
V0",IPROUTE1="iproute-1",IPROUTE2="iproute-2",IPADDR2="IP_Addr2",PEERADDR2="10.121.2.42"
prov-add:EISUPPATH:NAME="eisup-hsi-ent2a",DESC="eisup-hsi-ent2a",EXTNODE="hsi-ent2a",MDO="
EISUP",CUSTGRPID="ICCM",ORIGLABEL="",TERMLABEL=""
prov-add:MGCPPATH:NAME="mgcp-as5400-ent2a",DESC="MGCP path for
as5400-ent2a",EXTNODE="as5400-ent2a"
prov-add:MGCPPATH:NAME="mgcp-as5400-ent2b",DESC="MGCP path for
as5400-ent2b",EXTNODE="as5400-ent2b"
prov-add:LNKSET:NAME="lnkset-pstn1",DESC="pstn1
lnkset",APC="pstn1",PROTO="SS7-UK",TYPE="IP"
prov-add:IPLNK:NAME="hsi-ent2a-iplnk-1",DESC="hsi-ent2a-iplnk-1",SVC="eisup-hsi-ent2a",IPA
DDR="IP_Addr1",PORT=8003,PEERADDR="10.120.2.31",PEER
PORT=8003,PRI=1,IPROUTE="iproute-1"
prov-add:IPLNK:NAME="hsi-ent2a-iplnk-2",DESC="hsi-ent2a-iplnk-2",SVC="eisup-hsi-ent2a",IPA
DDR="IP_Addr2",PORT=8003,PEERADDR="10.121.2.31",PEER
PORT=8003,PRI=2,IPROUTE="iproute-2"
prov-add:IPLNK:NAME="as5400-ent2a-iplnk1",DESC="IP link 1 to
as5400-ent2a",SVC="mgcp-as5400-ent2a",IPADDR="IP_Addr1",PORT=2427,PEERADDR="10.12
0.2.21",PEERPORT=2427,PRI=1,IPROUTE="iproute-1"
prov-add:IPLNK:NAME="as5400-ent2a-iplnk2",DESC="IP link 2 to
as5400-ent2a",SVC="mgcp-as5400-ent2a",IPADDR="IP_Addr2",PORT=2427,PEERADDR="10.12
1.2.21",PEERPORT=2427,PRI=2,IPROUTE="iproute-2"
prov-add:IPLNK:NAME="as5400-ent2b-iplnk1",DESC="IP link 1 to
as5400-ent2b",SVC="mgcp-as5400-ent2b",IPADDR="IP_Addr1",PORT=2427,PEERADDR="10.12
0.2.22",PEERPORT=2427,PRI=1,IPROUTE="iproute-1"
prov-add:IPLNK:NAME="as5400-ent2b-iplnk2",DESC="IP link 2 to
as5400-ent2b",SVC="mgcp-as5400-ent2b",IPADDR="IP_Addr2",PORT=2427,PEERADDR="10.12
1.2.22",PEERPORT=2427,PRI=2,IPROUTE="iproute-2"
prov-add:SS7ROUTE:NAME="ss7r-pstn1",DESC="SS7 Route to
pstn1",OPC="opc",DPC="pstn1",LNKSET="lnkset-pstn1",PRI=1
prov-add:C7IPLNK:NAME="pstn1-c7lnk-1",DESC="C7 IP link 1 to
pstn1",LNKSET="lnkset-pstn1",SLC=0,PRI=1,TIMESLOT=0,SESSIONSET="sset-slt-ent2a"
prov-add:C7IPLNK:NAME="pstn1-c7lnk-2",DESC="C7 IP link 2 to
pstn1",LNKSET="lnkset-pstn1",SLC=1,PRI=1,TIMESLOT=0,SESSIONSET="sset-slt-ent2b"
prov-add:PROFILE:NAME="lvl2cmpf-1001",TYPE="commonprofile",clli="HSI"
prov-add:PROFILE:NAME="lvl1eisupf-1001",TYPE="eisupprofile",commonprofile="lvl2cmpf-1001",
custgrpid="ICCM"
prov-add:DNSPARAM:CacheSize="500",DnsServer1="0.0.0.0",DnsServer2="0.0.0.0",KeepAlive="30"
,Policy="HIERARCHY",QueryTimeout="1000",TTL="3600"
prov-add:TOS:DSCP = "CS3"
prov-ed:accrespcat:name="default",acl1drcant=50,acl1drskip=20,acl1arcant=50,acl1arskip=20,
acl2drcant=90,acl2drskip=10,acl2arcant=90,acl2arskip
=10,acl3drcant=100,acl3drskip=0,acl3arcant=100,acl3arskip=0
prov-ed:mclcallreject:name="mcl1",callreject=25
prov-ed:mclcallreject:name="mcl2",callreject=50
prov-ed:mclcallreject:name="mcl3",callreject=100
prov-ed:mclthreshold:name="callrate",mcl1onset=0,mcl1abate=0,mcl2onset=0,mcl2abate=0,mcl3o
nset=0,mcl3abate=0
prov-ed:mclthreshold:name="cpu",mcl1onset=82,mcl1abate=75,mcl2onset=90,mcl2abate=77,mcl3on
set=95,mcl3abate=85
prov-ed:mclthreshold:name="memoryaddress",mcl1onset=84,mcl1abate=80,mcl2onset=88,mcl2abate
=82,mcl3onset=93,mcl3abate=85
prov-ed:mclthreshold:name="queuelen",mcl1onset=75,mcl1abate=60,mcl2onset=80,mcl2abate=70,m
cl3onset=85,mcl3abate=75
prov-ed:mclthreshold:name="virtualmemory",mcl1onset=80,mcl1abate=75,mcl2onset=85,mcl2abate
=80,mcl3onset=90,mcl3abate=80
prov-dlt:inservice:name="ansi-ain-800-npa"
prov-dlt:inservice:name="ansi-ain-800-npa-nxx"
```

```
prov-dlt:inservice:name="ansi-ain-800-npanxxx"
prov-dlt:inservice:name="ansi-ain-800-ti"
prov-dlt:inservice:name="ansi-pre-ain-800"
prov-dlt:inservice:name="ansi-pre-ain-800-ssn"
prov-dlt:inservice:name="ansi-pre-ain-800-ti"
prov-dlt:inservice:name="ansi-pre-ain-800-ts"
prov-dlt:inservice:name="c1-lnp"
prov-dlt:inservice:name="cs1-inap-cli-initdp"
prov-dlt:inservice:name="cs1i-nap-cli-srr"
prov-dlt:inservice:name="generic-lnp"
prov-dlt:inservice:name="genesys-800"
prov-dlt:inservice:name="inap-freephon-initdp"
prov-dlt:inservice:name="inap-lnp-initdp"
prov-dlt:inservice:name="inap-lnp-norway"
prov-dlt:inservice:name="inap-lnp-portugal"
prov-dlt:inservice:name="inap-pp-bcsm"
prov-dlt:inservice:name="inap-pp-charge-atexp"
prov-dlt:inservice:name="inap-pp-charge-final"
prov-dlt:inservice:name="inap-pp-charge-texp"
prov-dlt:inservice:name="inap-pp-initdp"
prov-dlt:inservice:name="inap-precarr-initdp"
prov-dlt:inservice:name="inap-cs1-initdp"
prov-dlt:inservice:name="inap-cs1-dummy-25"
prov-dlt:inservice:name="inap-cs1-dummy-26"
prov-dlt:inservice:name="inap-cs1-dummy-27"
prov-dlt:inservice:name="inap-cs1-dummy-28"
prov-dlt:inservice:name="inap-cs2-initdp"
prov-dlt:inservice:name="ansi-pre-ain-cnam"
prov-add:inservice:name="ansi-ain-800-npa",skortcv=4,gtorssn="ROUTEBYGT",gtformat="GTTT",m
sname="ansi-ain-800-npa"
prov-add:inservice:name="ansi-ain-800-npa-nxx",skortcv=5,gtorssn="ROUTEBYGT",gtformat="GTT
T",msname="ansi-ain-800-npa-nxx"
prov-add:inservice:name="ansi-ain-800-npanxxx",skortcv=8,gtorssn="ROUTEBYGT",gtformat="GTT
T",msname="ansi-ain-800-npanxxx"
prov-add:inservice:name="ansi-ain-800-ti",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT",ms
name="ansi-ain-800-ti"
prov-add:inservice:name="ansi-pre-ain-800",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT",m
sname="ansi-pre-ain-800"
prov-add:inservice:name="ansi-pre-ain-800-ssn",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NO
GT",msname="ansi-pre-ain-800-ssn"
prov-add:inservice:name="ansi-pre-ain-800-ti",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT
",msname="ansi-pre-ain-800-ti"
prov-add:inservice:name="ansi-pre-ain-800-ts",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="ansi-pre-ain-800-ts"
prov-add:inservice:name="ansi-pre-ain-cnam",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT",
msname="ansi-pre-ain-cnam"
prov-add:inservice:name="c1-lnp",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT",msname="c1-
lnp"
prov-add:inservice:name="cs1-inap-cli-initdp",skortcv=1,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="cs1-inap-cli-initdp"
prov-add:inservice:name="cs1i-nap-cli-srr",skortcv=1,gtorssn="ROUTEBYSSN",gtformat="NOGT",
msname="cs1i-nap-cli-srr"
prov-add:inservice:name="generic-lnp",skortcv=37,gtorssn="ROUTEBYGT",gtformat="GTTT",msnam
e="generic-lnp"
prov-add:inservice:name="genesys-800",skortcv=0,gtorssn="ROUTEBYGT",gtformat="GTTT",msname
="genesys-800"
prov-add:inservice:name="inap-cs1-dummy-25",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT"
,msname="inap-cs1-dummy-25"
prov-add:inservice:name="inap-cs1-dummy-26",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT"
,msname="inap-cs1-dummy-26"
prov-add:inservice:name="inap-cs1-dummy-27",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT"
,msname="inap-cs1-dummy-27"
prov-add:inservice:name="inap-cs1-dummy-28",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT"
,msname="inap-cs1-dummy-28"
```

```
prov-add:inservice:name="inap-cs1-initdp",skortcv=90001,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="inap-cs1-initdp"
prov-add:inservice:name="inap-cs2-initdp",skortcv=90001,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="inap-cs2-initdp"
prov-add:inservice:name="inap-freephon-initdp",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NO
GT",msname="inap-freephon-initdp"
prov-add:inservice:name="inap-lnp-initdp",skortcv=1,gtorssn="ROUTEBYSSN",gtformat="NOGT",m
sname="inap-lnp-initdp"
prov-add:inservice:name="inap-lnp-norway",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT",m
sname="inap-lnp-norway"
prov-add:inservice:name="inap-lnp-portugal",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT"
,msname="inap-lnp-portugal"
prov-add:inservice:name="inap-pp-bcsm",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOGT",msna
me="inap-pp-bcsm"
prov-add:inservice:name="inap-pp-charge-atexp",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NO
GT",msname="inap-pp-charge-atexp"
prov-add:inservice:name="inap-pp-charge-final",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NO
GT",msname="inap-pp-charge-final"
prov-add:inservice:name="inap-pp-charge-texp",skortcv=0,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="inap-pp-charge-texp"
prov-add:inservice:name="inap-pp-initdp",skortcv=1,gtorssn="ROUTEBYSSN",gtformat="NOGT",ms
name="inap-pp-initdp"
prov-add:inservice:name="inap-precarr-initdp",skortcv=2,gtorssn="ROUTEBYSSN",gtformat="NOG
T",msname="inap-precarr-initdp"
prov-add:sigsvcprop:NAME="eisup-hsi-ent2a",H323AdjunctLink="1"
prov-add:sigsvcprop:NAME="mgcp-as5400-ent2a",mgcpDomainNameRemote="s2/ds1-0/1@AS5400-ENT2A
"
prov-add:sigsvcprop:NAME="mgcp-as5400-ent2b",mgcpDomainNameRemote="s2/ds1-0/1@AS5400-ENT2B
"
prov-add:files:name="tkgfile",file="Static_12_05/export_trkgrp.dat",action="IMPORT"
prov-add:TRNKGRPPROF:name="1001",profile="lvl1eisupf-1001"
prov-add:files:name="bcfile",file="Static_12_05/export_trunk.dat",action="IMPORT"
```

Routing.mml

```
prov-add:rttrnkgrp:name="1001",type=4,reattempts=0,queuing=0,cutthrough=2,resincperc=0
prov-add:rttrnkgrp:name="2001",type=1,reattempts=2,queuing=0,cutthrough=2,resincperc=0
prov-add:rttrnk:weightedTG="OFF",name="route2hsi",trnkgrpnum=1001
prov-add:rttrnk:weightedTG="OFF",name="route2pstn",trnkgrpnum=2001
prov-add:rtlist:name="rtlist2pstn44",rtname="route2pstn",distrib="OFF"
prov-add:rtlist:name="rtlist2hsi",rtname="route2hsi",distrib="OFF"
3.4.3 ICCM.mml
numan-add:dialplan:custgrpid="ICCM", OVERDEC="YES"
numan-ed: resulttable: custgrpid="ICCM", name="CSCOADRST1", resulttype="RETRY_ACTION",
dw1="Reattempt", dw2="0",setname="CSCOADRST1"
numan-ed: resulttable: custgrpid="ICCM", name="CSCOADRST2", resulttype="RETRY_ACTION",
dw1="Redirect",dw2="0",setname="CSCOADRST2"
numan-ed:cause:custgrpid="ICCM",causevalue=1,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=11,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=26,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=29,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=38,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=41,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=44,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=49,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=50,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=58,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=69,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=87,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=94,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=107,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ICCM",causevalue=118,setname="CSCOADRST1"
```

```
numan-ed:cause:custgrpid="ICCM",causevalue=145,setname="CSCOADRST2"
```

ILGW.mml

```
numan-add:dialplan:custgrpid="ILGW", OVERDEC="YES"
numan-ed: resulttable: custgrpid="ILGW", name="CSCOADRST1", resulttype="RETRY_ACTION",
dw1="Reattempt",dw2="0",setname="CSCOADRST1"
numan-ed: resulttable: custgrpid="ILGW", name="CSCOADRST2", resulttype="RETRY_ACTION",
dw1="Redirect",dw2="0",setname="CSCOADRST2"
numan-ed:cause:custgrpid="ILGW",causevalue=1,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=11,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=26,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=29,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=38,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=41,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=44,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=49,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=50,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=58,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=69,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=87,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=94,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=107,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=118,setname="CSCOADRST1"
numan-ed:cause:custgrpid="ILGW",causevalue=145,setname="CSCOADRST2"
```

Properties.dat

```
eisup-hsi-ent2a.H323AdjunctLink = 1
mgcp-as5400-ent2a.mgcpDomainNameRemote = s2/ds1-0/1@AS5400-ENT2A
mgcp-as5400-ent2b.mgcpDomainNameRemote = s2/ds1-0/1@AS5400-ENT2B
ss7-u-1.chkPtPort = 2001
tg-1001.AllowH323Hairpin = 1
tg-1001.CLLI = HSI
tg-1001.CustGrpId = ICCM
tg-1001.commonProfile = lvl2cmpf-1001
tg-2001.CLLI = PSTN1
tg-2001.FAXsupport = 1
tg-2001.GatewayRBToneSupport = 1
```

Note Default properties prefixed by an "*", SS7-<ver>.<property_name> properties, and TALI-IOCC.<property_name> properties, are not shown

Export_trkgrp.dat

```
<!--#xml - 9.8001-->
<trunk-groups>
<version base="9.8001" revision="0"/>
<trunkgroup name="1001" type="IP" svc="eisup-hsi-ent2a" clli="HSI" selseq="LIDL" qable="N"
origlabel="0" termlabel="0">
<property name="CustGrpId">ICCM</property>
<property name="default">0</property>
</trunkgroup>
<trunkgroup name="2001" type="TDM_ISUP" svc="ss7p-pstn1" clli="PSTN1" selseq="LIDL"
qable="N" origlabel="0" termlabel="0">
<property name="GatewayRBToneSupport">1</property>
<property name="FAXsupport">1</property>
<property name="default">0</property>
```

```
</trunkgroup>
</trunk-groups>
```

Export_trunk.dat

```
#format3 - 0.0
2001 1 ffff 1 as5400-ent2a s2/ds1-0/1@as5400-ent2a
2001 2 ffff 2 as5400-ent2a s2/ds1-0/2@as5400-ent2a
2001 3 ffff 3 as5400-ent2a s2/ds1-0/3@as5400-ent2a
2001 4 ffff 4 as5400-ent2a s2/ds1-0/4@as5400-ent2a
2001 6 ffff 6 as5400-ent2a s2/ds1-0/6@as5400-ent2a
2001 7 ffff 7 as5400-ent2a s2/ds1-0/7@as5400-ent2a
2001 8 ffff 8 as5400-ent2a s2/ds1-0/8@as5400-ent2a
2001 9 ffff 9 as5400-ent2a s2/ds1-0/9@as5400-ent2a
2001 10 ffff 10 as5400-ent2a s2/ds1-0/10@as5400-ent2a
2001 11 ffff 11 as5400-ent2a s2/ds1-0/11@as5400-ent2a
2001 12 ffff 12 as5400-ent2a s2/ds1-0/12@as5400-ent2a
2001 13 ffff 13 as5400-ent2a s2/ds1-0/13@as5400-ent2a
2001 14 ffff 14 as5400-ent2a s2/ds1-0/14@as5400-ent2a
2001 15 ffff 15 as5400-ent2a s2/ds1-0/15@as5400-ent2a
2001 16 ffff 16 as5400-ent2a s2/ds1-0/16@as5400-ent2a
2001 17 ffff 17 as5400-ent2a s2/ds1-0/17@as5400-ent2a
2001 18 ffff 18 as5400-ent2a s2/ds1-0/18@as5400-ent2a
2001 19 ffff 19 as5400-ent2a s2/ds1-0/19@as5400-ent2a
2001 20 ffff 20 as5400-ent2a s2/ds1-0/20@as5400-ent2a
2001 21 ffff 21 as5400-ent2a s2/ds1-0/21@as5400-ent2a
2001 22 ffff 22 as5400-ent2a s2/ds1-0/22@as5400-ent2a
2001 23 ffff 23 as5400-ent2a s2/ds1-0/23@as5400-ent2a
2001 24 ffff 24 as5400-ent2a s2/ds1-0/24@as5400-ent2a
2001 25 ffff 25 as5400-ent2a s2/ds1-0/25@as5400-ent2a
2001 26 ffff 26 as5400-ent2a s2/ds1-0/26@as5400-ent2a
2001 27 ffff 27 as5400-ent2a s2/ds1-0/27@as5400-ent2a
2001 28 ffff 28 as5400-ent2a s2/ds1-0/28@as5400-ent2a
2001 29 ffff 29 as5400-ent2a s2/ds1-0/29@as5400-ent2a
2001 30 ffff 30 as5400-ent2a s2/ds1-0/30@as5400-ent2a
```

XECfgParm.dat

This update to XECfgParm.dat is required for overlap support of PBX gateways (specifically required for the support of DPNSS):

```
*.analysisCapabilityLevel = 1
```

Full Number Translation with TimesTen Database

The Full Number Translations feature provides a large-scale, number translation function on the Cisco PGW. This feature enhances the current PGW database query mode, which is used for local number portability (LNP) and CLI screening, by handling contiguous ranges of numbers with analysis and modification capabilities. The Full Number Translations feature supports large-scale changes of individual numbers. This feature adds the NUM_TRANS result type that is implemented in analysis where the existing Times Ten database is used to store the dial plan numbers.

The full number replacement mechanism adds a general number replacement result type, NUM_TRANS, available for A-number and B-number analysis. In addition, a Times Ten query and full number translation table are also added.

The Full Number Translation with TimesTen Database feature is introduced from Hosted UCS 6.1(a) onwards. This means that the association of E.164 numbers to Internal numbers will use this feature instead of configuring via mml.

This section includes the following toopics:

Sparc Based Platform Configuration

Opteron Based Platform Configuration

Sparc Based Platform Configuration

In order to use this feature, HUCSprovx10 script need to be uploaded on the PGW.

Procedure:

Step 1 Upload the HUCS_x10_package.gz package onto a FTP server reachable by the PGW.

Step 2 Log into the PGW as the PGW application user (default is mgcusr).

Step 3 Download HUCS_x10_package.gz from the FTP server into /opt/CiscoMGC/local.

Step 4 Unzip HUCS_x10_package.gz, for example **gunzip HUCS_x10_package.gz.**

Step 5 Untar HUCS_x10_package, for example **tar -xvf HUCS_x10_package.**

The following output is displayed:

```
x ./HUCS_x10, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_vm64, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_vm64/jdk64-sparc-1_5_0_06.gz, 9424713 bytes, 18408 tape blocks
x ./HUCS_x10/java_vm64/jdk64-amd64-1_5_0_06.gz, 5439360 bytes, 10624 tape blocks
x ./HUCS_x10/java_appl, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/data, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/data/fnt_sample_data, 180 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/data/lnp_fnt_sample_data, 246 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/data/lnp_sample_data, 67 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/bin, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/bin/HUCSprovx10, 246 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/bin/HUCSprovx10.jar, 8143 bytes, 16 tape blocks
```

Step 6 Go to the java_vm64 folder, for example **cd HUCS_x10/java_vm64.**

Step 7 Unzip jdk64-sparc-1_5_0_06.gz, for example **gunzip jdk64-sparc-1_5_0_06.gz.**

Step 8 Untar jdk64-sparc-1_5_0_06, for example **tar -xvf jdk64-sparc-1_5_0_06.**

The following output is displayed:

```
x ./SUNWj5rtx, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/pkgmap, 7335 bytes, 15 tape blocks
x ./SUNWj5rtx/pkginfo, 571 bytes, 2 tape blocks
x ./SUNWj5rtx/install, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/install/copyright, 93 bytes, 1 tape blocks
x ./SUNWj5rtx/install/depend, 1063 bytes, 3 tape blocks
x ./SUNWj5rtx/reloc, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/java, 81440 bytes, 160 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/keytool, 74520 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/orbd, 74664 bytes, 146 tape blocks
```

```
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/pack200, 74552 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/policytool, 74536 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/rmid, 74520 bytes, 146 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/rmiregistry, 74520 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/servertool, 74520 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/tnameserv, 74696 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/sparcv9/unpack200, 205960 bytes, 403 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/java, 81440 bytes, 160 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/keytool, 74520 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/orbd, 74664 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/pack200, 74552 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/policytool, 74536 bytes, 146
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/rmid, 74520 bytes, 146 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/rmiregistry, 74520 bytes, 146
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/servertool, 74520 bytes, 146
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/tnameserv, 74696 bytes, 146
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/sparcv9/unpack200, 205960 bytes, 403
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/awt_robot, 26432 bytes, 52 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/gtkhelper, 7760 bytes, 16 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/headless, 0 bytes, 0 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/headless/libmawt.so, 40400
bytes, 79 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/jvm.cfg, 659 bytes, 2 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libJdbcOdbc.so, 56552 bytes,
111 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libawt.so, 1057000 bytes, 2065
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libcmm.so, 388400 bytes, 759
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libdcpr.so, 187368 bytes, 366
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libdt_socket.so, 19560 bytes,
39 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libfontmanager.so, 479320
bytes, 937 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libhprof.so, 292680 bytes, 572
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libinstrument.so, 86784 bytes,
170 tape blocks
```

```
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libioser12.so, 14568 bytes, 29
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libj2pkcs11.so, 66144 bytes,
130 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjaas_unix.so, 7344 bytes, 15
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjava.so, 179264 bytes, 351
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjava_crw_demo.so, 46616
bytes, 92 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjawt.so, 3160 bytes, 7 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWcg6.so, 11224 bytes,
22 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWffb.so, 11632 bytes,
23 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWm64.so, 7912 bytes,
16 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdwp.so, 336848 bytes, 658
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjpeg.so, 204264 bytes, 399
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsig.so, 14264 bytes, 28
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsound.so, 329360 bytes, 644
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsoundsolmidi.so, 20872
bytes, 41 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmanagement.so, 29040 bytes,
57 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmlib_image.so, 1370616
bytes, 2677 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmlib_image_v.so, 1870136
bytes, 3653 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libnet.so, 84240 bytes, 165
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libnio.so, 34024 bytes, 67 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/librmi.so, 2840 bytes, 6 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libsaproc.so, 49280 bytes, 97
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libsunwjdga.so, 10304 bytes, 21
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libunpack.so, 95064 bytes, 186
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libverify.so, 82200 bytes, 161
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libxinerama.so, 9832 bytes, 20
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libzip.so, 83568 bytes, 164
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/motif21, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/motif21/libmawt.so, 607480
bytes, 1187 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/native_threads, 0 bytes, 0 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/native_threads/libhpi.so, 47832
bytes, 94 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/Xusage.txt, 1423 bytes,
3 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/libjvm.so, 12163008
bytes, 23756 tape blocks
```

```
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/libjvm_db.so, 46656
bytes, 92 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/xawt, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/sparcv9/xawt/libmawt.so, 257176 bytes,
503 tape blocks
```

Step 9 Add the **SUNWj5rtx** package, for example **pkgadd -d . SUNWj5rtx.**

The following output is displayed:

```
Processing package instance <SUNWj5rtx> from </opt/CiscoMGC/local/HUCS_x10/java_vm64>
JDK 5.0 64-bit Runtime Env. (1.5.0_06)(sparc) 1.5.0,REV=2004.12.06.22.09
Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
Use is subject to license terms.
Using </usr> as the package base directory.
## Processing package information.
## Processing system information.
   7 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
Installing JDK 5.0 64-bit Runtime Env. (1.5.0_06) as <SUNWj5rtx>
## Installing part 1 of 1.
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/java
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/keytool
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/orbd
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/pack200
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/policytool
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/rmid
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/rmiregistry
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/servertool
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/tnameserv
/usr/jdk/instances/jdk1.5.0/bin/sparcv9/unpack200
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/java
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/keytool
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/orbd
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/pack200
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/policytool
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/rmid
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/rmiregistry
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/servertool
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/tnameserv
/usr/jdk/instances/jdk1.5.0/jre/bin/sparcv9/unpack200
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/awt_robot
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/gtkhelper
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/headless/libmawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/jvm.cfg
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libJdbcOdbc.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libcmm.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libdcpr.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libdt_socket.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libfontmanager.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libhprof.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libinstrument.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libioser12.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libj2pkcs11.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjaas_unix.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjava.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjava_crw_demo.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWafb.so <symbolic link>
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWcg6.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWffb.so
```

```
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdgaSUNWm64.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjdwp.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjpeg.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsig.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsound.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libjsoundsolmidi.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmanagement.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmlib_image.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libmlib_image_v.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libnet.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libnio.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/librmi.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libsaproc.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libsunwjdga.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libunpack.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libverify.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libxinerama.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/libzip.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/motif21/libmawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/native_threads/libhpi.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/Xusage.txt
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/libjsig.so <symbolic link>
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/libjvm.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/server/libjvm_db.so
/usr/jdk/instances/jdk1.5.0/jre/lib/sparcv9/xawt/libmawt.so
[ verifying class <none> ]
Installation of <SUNWj5rtx> was successful.
```

Step 10 Go to **/opt/CiscoMGC/local/HUCS_x10/java_appl/bin**.

Step 11 Move HUCSprovx10 and HUCSprovx10.jar to /opt/CiscoMGC/local/, for example: **mv HUCS* /opt/CiscoMGC/local**

Opteron Based Platform Configuration

In order to use this feature, HUCSprovx10 script need to be uploaded on the PGW.

Procedure:

Step 1 Upload the HUCS_x10_package.gz package onto a FTP server reachable by the PGW.

Step 2 Log into the PGW as the PGW application user (default is mgcusr).

Step 3 Download HUCS_x10_package.gz from the FTP server into /opt/CiscoMGC/local.

Step 4 Unzip HUCS_x10_package.gz, for example **gunzip HUCS_x10_package.gz.**

Step 5 Untar HUCS_x10_package, for example **tar -xvf HUCS_x10_package.**

The following output is displayed:

```
x ./HUCS_x10, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_vm64, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_vm64/jdk64-sparc-1_5_0_06.gz, 9424713 bytes, 18408 tape blocks
x ./HUCS_x10/java_vm64/jdk64-amd-1_5_0_06.gz, 5439360 bytes, 10624 tape blocks
x ./HUCS_x10/java_appl, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/data, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/data/fnt_sample_data, 180 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/data/lnp_fnt_sample_data, 246 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/data/lnp_sample_data, 67 bytes, 1 tape blocks
x ./HUCS_x10/java_appl/bin, 0 bytes, 0 tape blocks
x ./HUCS_x10/java_appl/bin/HUCSprovx10, 246 bytes, 1 tape blocks
```

```
x ./HUCS_x10/java_appl/bin/HUCSprovx10.jar, 8118 bytes, 16 tape blocks
```

Step 6 Go to the java_vm64 folder, for example **cd HUCS_x10/java_vm64.**

Step 7 Unzip jdk64-amd-1_5_0_06.gz, for example **gunzip jdk64-amd-1_5_0_06.gz.**

Step 8 Untar jdk64-amd-1_5_0_06, for example **tar -xvf jdk64-amd-1_5_0_06.**

The following output is displayed:

```
x ./SUNWj5rtx, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/pkgmap, 6599 bytes, 13 tape blocks
x ./SUNWj5rtx/pkginfo, 573 bytes, 2 tape blocks
x ./SUNWj5rtx/install, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/install/copyright, 93 bytes, 1 tape blocks
x ./SUNWj5rtx/install/depend, 1063 bytes, 3 tape blocks
x ./SUNWj5rtx/reloc, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/java, 68016 bytes, 133 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/keytool, 71424 bytes, 140 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/orbd, 71568 bytes, 140 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/pack200, 71456 bytes, 140 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/policytool, 71456 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/rmid, 71424 bytes, 140 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/rmiregistry, 71424 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/servertool, 71424 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/tnameserv, 71600 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/bin/amd64/unpack200, 200368 bytes, 392 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/java, 68016 bytes, 133 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/keytool, 71424 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/orbd, 71568 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/pack200, 71456 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/policytool, 71456 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/rmid, 71424 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/rmiregistry, 71424 bytes, 140
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/servertool, 71424 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/tnameserv, 71600 bytes, 140 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/bin/amd64/unpack200, 200368 bytes, 392 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/awt_robot, 24768 bytes, 49 tape
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/gtkhelper, 7120 bytes, 14 tape
blocks
```

```
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/headless, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/headless/libmawt.so, 33024 bytes, 
65 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/j2pkcs11.dll, 65666 bytes, 129 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/j2pkcs11_g.dll, 82054 bytes, 161 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/jvm.cfg, 652 bytes, 2 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libJdbcOdbc.so, 64768 bytes, 127 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libawt.so, 481776 bytes, 941 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libcmm.so, 383216 bytes, 749 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libdcpr.so, 190656 bytes, 373 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libdt_socket.so, 18072 bytes, 36 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libfontmanager.so, 457896 bytes, 
895 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libhprof.so, 179616 bytes, 351 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libinstrument.so, 74152 bytes, 
145 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libioser12.so, 16824 bytes, 33 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libj2pkcs11.so, 61192 bytes, 120 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjaas_unix.so, 6232 bytes, 13 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjava.so, 163928 bytes, 321 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjava_crw_demo.so, 26160 bytes, 
52 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjawt.so, 3432 bytes, 7 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjdwp.so, 278624 bytes, 545 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjpeg.so, 187080 bytes, 366 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjsig.so, 14824 bytes, 29 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libjsound.so, 294688 bytes, 576 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libmanagement.so, 27448 bytes, 54 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libmlib_image.so, 807296 bytes, 
1577 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libnet.so, 71744 bytes, 141 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libnio.so, 30816 bytes, 61 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/librmi.so, 3056 bytes, 6 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libsaproc.so, 62024 bytes, 122 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libunpack.so, 95712 bytes, 187 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libverify.so, 63232 bytes, 124 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/libzip.so, 75200 bytes, 147 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/motif21, 0 bytes, 0 tape blocks
```

```
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/motif21/libmawt.so, 528728 bytes, 
1033 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/native_threads, 0 bytes, 0 tape 
blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/native_threads/libhpi.so, 41312 
bytes, 81 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/server, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/server/Xusage.txt, 1423 bytes, 3 
tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/server/libjvm.so, 12230144 bytes, 
23887 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/server/libjvm_db.so, 54776 bytes, 
107 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/xawt, 0 bytes, 0 tape blocks
x ./SUNWj5rtx/reloc/jdk/instances/jdk1.5.0/jre/lib/amd64/xawt/libmawt.so, 226704 bytes, 
443 tape blocks
```

Add the SUNWj5rtx package, for example **pkgadd -d . SUNWj5rtx**

The following output is displayed:

```
Processing package instance <SUNWj5rtx> from </opt/CiscoMGC/local/HUCS_x10/java_vm64>
JDK 5.0 64-bit Runtime Env. (1.5.0_06)(i386) 1.5.0,REV=2005.03.04.02.15
Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
Use is subject to license terms.
Using </usr> as the package base directory.
## Processing package information.
## Processing system information.
   7 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

Installing JDK 5.0 64-bit Runtime Env. (1.5.0_06) as <SUNWj5rtx>
## Installing part 1 of 1.
/usr/jdk/instances/jdk1.5.0/bin/amd64/java
/usr/jdk/instances/jdk1.5.0/bin/amd64/keytool
/usr/jdk/instances/jdk1.5.0/bin/amd64/orbd
/usr/jdk/instances/jdk1.5.0/bin/amd64/pack200
/usr/jdk/instances/jdk1.5.0/bin/amd64/policytool
/usr/jdk/instances/jdk1.5.0/bin/amd64/rmid
/usr/jdk/instances/jdk1.5.0/bin/amd64/rmiregistry
/usr/jdk/instances/jdk1.5.0/bin/amd64/servertool
/usr/jdk/instances/jdk1.5.0/bin/amd64/tnameserv
/usr/jdk/instances/jdk1.5.0/bin/amd64/unpack200
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/java
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/keytool
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/orbd
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/pack200
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/policytool
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/rmid
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/rmiregistry
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/servertool
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/tnameserv
/usr/jdk/instances/jdk1.5.0/jre/bin/amd64/unpack200
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/awt_robot
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/gtkhelper
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/headless/libmawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/j2pkcs11.dll
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/j2pkcs11_g.dll
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/jvm.cfg
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libJdbcOdbc.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libcmm.so
```

```
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libdcpr.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libdt_socket.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libfontmanager.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libhprof.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libinstrument.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libioser12.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libj2pkcs11.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjaas_unix.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjava.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjava_crw_demo.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjdwp.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjpeg.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjsig.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libjsound.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libmanagement.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libmlib_image.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libnet.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libnio.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/librmi.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libsaproc.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libunpack.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libverify.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/libzip.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/motif21/libmawt.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/native_threads/libhpi.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/server/Xusage.txt
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/server/libjsig.so <symbolic link>
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/server/libjvm.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/server/libjvm_db.so
/usr/jdk/instances/jdk1.5.0/jre/lib/amd64/xawt/libmawt.so
[ verifying class <none> ]
Installation of <SUNWj5rtx> was successful.
```

Step 9 Go to **/opt/CiscoMGC/local/HUCS_x10/java_appl/bin**.

Step 10 Move HUCSprovx10 and HUCSprovx10.jar to /opt/CiscoMGC/local/, for example **mv HUCS* /opt/CiscoMGC/local.**

Cisco HSI Static Configuration

This section describes the required setup on the Cisco HSI before loading the USM platform.

Cisco HSI enables the Cisco PGW to talk to the Unified CM using H.323 via the H.323 gatekeeper. The HSI is an adjunct to the Cisco PGW and simply provides an H.323 interface.

For further information, refer to the Cisco H.323 Signaling Interface User Guide, Release 4.3.

Use the following HUCS specific static configuration settings on all HSIs:

RAS Parameters

- prov-add:name=ras,gatekeeperId=**HUCS_ZONE**
- prov-add:name=ras,gateway.prefix[1]=**999#**
- prov-add:name=ras,manualDiscovery.ipAddress=<gatekeeper_ip_address>, for example prov-add:name=ras,manualDiscovery.ipAddress=**10.120.4.51**
- prov-add:name=ras,manualDiscovery.port=**1719**

- prov-add:name=ras,terminalAlias[1].h323ID=<hsi_name>, for example prov-add:name=ras,terminalAlias[1].h323ID=**hsi-ent4a@ipcbuemea.cisco.com**

T.38 fax support

- prov-add:name=sys_config_static,t38maxval="**MaxBit 0x90, FxMaxBuf 0xc8, FxMaxData 0x48**"
- prov-add:name=sys_config_static,t38options="**FxFillBit 0, FxTransMMR 0, FxTransJBIG 0, FxRate Trans, FxUdpEC Red**"

DTMF support

- prov-add:name=sys_config_static, dtmfsupporteddirection=**both**
- prov-add:name=sys_config_static, dtmfsupportedtype=**dtmf**

Support for the transit of the redirecting number parameter (contained in Cisco Unified CM H.225 setup messages-nonStandardControl field)

- prov-add:name=sys_config_static, h225pavosupported=**enabled**

CLIP/CLIR support

- prov-add:name=SYS_CONFIG_STATIC,ClipClirSupported=**enabled**
- prov-add:name=CCPackage,A_CC_AnumDataSI=**1**
- prov-add:name=CCPackage,A_CC_Clir=**1**

Cisco Gatekeeper Static Configuration

This section describes the required setup on the Cisco Gatekeepers before loading the USM platform.

An H.323 gatekeeper is included in the HUCS platform to provide basic infrastructure capabilities. It provides registration capability for the Cisco PGW (via the Cisco HSI), Cisco Unified CM, and any H.323 customer devices. The gatekeeper forces all routing to use the Cisco PGW rather than to operate between Unified CM clusters.

Configure the following static configuration settings on the gatekeepers in global configuration mode:

- gatekeeper
- zone local HUCS_ZONE ipcbuemea.cisco.com
- gw-type-prefix 999#* default-technology
- no shutdown

CHAPTER 3

Defining and Configuring Core Network Elements and Resources

This chapter describes the required steps to define and configure core resources and network elements, how the components are associated to each other, and how Cisco PGWs and Cisco Unified CMs are configured for the first time. It includes the following sections:

Provider Administration

This section describes the required steps to define providers and various resources, such as number types and quantities, phone types and quantities, and so on. All Hosted UCS resources, network elements, countries, and the inventory of E.164 numbers, IP addresses, and phones are defined at the provider level. They can then be assigned to resellers, customers, customer divisions, and customer locations.

This section includes the following topics:

- Enabling USM User Roaming, page 3-4

Adding Providers

You can define multiple providers.

To create a provider, perform the following steps:

Procedure

Step 1 Choose **Provider Administration > Providers**.

Step 2 Click **Add**.

Step 3 From the Details menu, define the fields required for your implementation. The following fields are required, at the minimum, when adding a provider:

- Name—<*ProviderName*>; for example; **UKProvider**
- Address1—<*Address*>
- City—<*City*>
- Country—<*Country*>
- Post/Zip Code—<*Post/Zip Code*>
- Contact Name—<*ContactName*>
- Contact Telephone Number—<*ContactTelephoneNumber*>

Step 4 From the Hardware Set menu, enter the following:

- Type of Hardware Deployed—**HUCS: HUCS Sample Hardware Set: HUCS DIAL PLAN**
- From the GUI Branding menu, define the type of branding required.
- Branding of User Interface—Default GUI branding
- Check the **Default GUI branding** check box.

Step 5 Click **Add**.

Repeat this procedure for all providers.

Managing Number Resources

You can increase or decrease the quantity of number types (DDI extensions, internal extensions, and so on) available to the provider.

To increase or decrease the quantity of number types, perform the following steps:

Procedure

Step 1 Choose **Provider Administration > Number Type Counters**.

Step 2 From the Number Types menu, enter the appropriate number of each of the following:

- DDI Extensions—**2000**

- Internal Extensions—**2000**
- Analog PSTN Lines—**2000**
- Incoming Lines—**2000**
- Outgoing Lines—**2000**
- Emergency Call Back Lines—**2000**

Step 3 Click **Modify**.

Repeat this procedure for all providers.

Managing Phone Resources

You can increase or decrease the quantity of phone types, such as the Cisco Unified IP Phone 7941 (SIP), the Cisco Unified IP Phone 7961 (SCCP), and so on, available to the provider.

To increase or decrease the quantity of phone types, perform the following steps:

Procedure

Step 1 Choose **Provider Administration > Phone Type Counters**.

Step 2 From the Phone Types and Quantities menu, adjust the quantity for all required phone types as required for the implementation.

Step 3 Click **Adjust Limits**.

Repeat this procedure for all providers.

Managing Services

You can increase or decrease the quantity of service types, such as voice mail, conferencing, and so on, available to the provider.

To increase or decrease the quantity of service types, perform the following steps:

Procedure

Step 1 Choose **Provider Administration > Service Type Counters.**

Step 2 From the Service Type menu, adjust the quantity for all service types as required for the implementation.

Step 3 Click **Adjust Limits**.

Repeat this procedure for all providers.

Enabling USM User Roaming

To enable the option to use USM for logging in during user roaming, you must enable the BVSMUserRoaming preference setting. Additional preferences are configured at the Customer level to enable this feature per customer.

To activate this preference, perform the following steps:

Step 1 Choose **Provider Administration > Providers**.

Step 2 Select a Provider for which you want to activate the feature.

Step 3 Click **Preferences**.

Step 4 Click **BVSMUserRoaming**.

Step 5 Tick the available checkbox to enable the setting.

Step 6 Click **Modify**.

Repeat this for all required Providers.

Defining and Associating Gatekeepers

To define and configure Cisco PGWs, you must define and associate a gatekeeper.

Defining Gatekeepers

A gatekeeper is defined in USM as a Cisco 36xx Series Router.

To define a gatekeeper, perform the following steps:

Procedure

Step 1 Choose **Network > Gatekeepers.**

Step 2 Click **Add**.

Step 3 Click **Add** next to Cisco36xx (Cisco 36xx Series Router).

Step 4 From the Details menu, enter the following:

- Host Name—<*uniquename*>; for example, **GK2600-ENT2A**
- IP Address—<*gatekeeperIP*>; for example, **10.120.2.51**
- Description—<*gatekeeperdescription*>; for example, **City 2 Gatekeeper A**
- Config Password—<*configpassword*>; for example, **cisco**
- Enable Password—<*enablepassword*>; for example, **cisco**
- Version—<*gatekeeperIOSversion*>; for example, **Cisco36xx: 12.x**

Step 5 Click **Add**.

Note In Hosted UCS 7.1(a), Gatekeepers are supported on various Router types, not only on 36xx Series Routes.

Repeat this procedure for all gatekeepers.

Associating Gatekeepers

In Hosted UCS 7.1(a) when multiple gatekeepers are used; they are configured in a cluster associated to each other.

To associate gatekeepers, perform the following steps:

Procedure

Step 1 Choose **Network > Gatekeepers.**

Step 2 Click **H323=>H323 Links** next to one of the gatekeepers you want to associate.

Step 3 Click **Connect** next to the gatekeeper you want to associate.

Defining and Associating Cisco PGW

To define and configure Cisco PGWs, you must define Cisco PGWs and associate them with gatekeepers.

Defining Cisco PGWs

The Cisco PGW is defined in USM as a transit switch.

To define a Cisco PGW, the following steps, at a minimum, are required.

Note Other steps, such as setting the congestion threshold, may be required for specific implementations.

Procedure

Step 1 Choose **Network > Transit Switches.**

Step 2 Click **Add**.

Step 3 Next to PGW (Cisco Transit Switch), click **Add**.

Step 4 From the Enter PGW Details menu, enter the following:

- Name—<*uniquename*>; for example, **PGW-ENT2**
- Description—<*pgwdescription*>; for example, **City 2 PGWs**
- Software Version—**PGW: 9.7.3**

- Line Capacity—<*linecapacity*>; for example, **30000**

Note This is set in stone and cannot be changed later

- Country—<*countrywherepgwis*>; for example, **United Kingdom**
- Call Processor ID (Default=AUTO)—**AUTO**
- Click **Detailed trace file of configuration sessions?**.

Step 5 From the Main PGW Server Details menu, enter the following:

- Host Name—<*mainpgwhostname*>; for example, **PGW-EN23M**
- Primary IP Address—<*primaryIP*>; for example, **10.120.2.11**
- Secondary IP Address—<*secondaryIP*>; for example, **10.121.2.11**
- Config Username—<*configusername*>; for example, **mgcusr**
- Config Password—<*configpassword*>; for example, **cisco**
- Config Prompt—**%**
- MML command—**mml –s8**
- FTP Path—**/opt/CiscoMGC/etc/cust_specific**

Step 6 From the Backup PGW Server Details menu, if one exists, enter the following:

- Host Name—<*backuppgwhostname*>; for example, **PGW-ENT2S**
- Primary IP Address—<*primaryIP*>; for example, **10.120.2.12**
- Secondary IP Address—<*secondaryIP*>; for example, **10.121.2.12**
- Config Username—<*configusername*>; for example, **mgcusr**
- Config Password—<*configpassword*>; for example, **cisco**
- Config Prompt—**%**
- MML command—**mml –s12**
- FTP Path—**/opt/CiscoMGC/etc/cust_specific**

Step 7 Click **Add**.

Note In Hosted UCS 7.1(a), PGW 9.8(1) is also supported in addition to PGW 9.6(1) and 9.7(3).

Repeat this procedure for all Cisco PGWs.

Associating Cisco PGWs with a Gatekeeper

To associate the Cisco PGW with the gatekeeper, perform the following steps:

Procedure

Step 1 Choose **Network > Transit Switches**.

Step 2 Click **Transit=>Gatekeeper** next to one of the Cisco PGWs you want to associate with the gatekeepers.

Step 3 Click **Connect** next to the gatekeeper you want to associate with the Cisco PGW.

Repeat this procedure for all Cisco PGWs.

Note If the gatekeepers are in a cluster, the Cisco PGW should be associated with only one of the gatekeepers in the cluster.

Defining and Configuring Cisco Unified CM Clusters

To define and configure Cisco Unified CM clusters, you must do the following:

- Adding Cisco Unified CM Clusters and Publisher Servers, page 3-7
- Adding Cisco Unified Communications Manager Subscriber Servers, page 3-8
- Define Cisco Unified Communications Manager Set, page 3-12
- Importing Softkey and Phone Button Templates, page 3-11
- Associating Cisco Unified Communications Manager Clusters with Gatekeepers, page 3-11

Adding Cisco Unified CM Clusters and Publisher Servers

Cisco Unified CM is defined in USM as a PBX device.

To define a Cisco Unified CM cluster and the publisher server, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Click **Add**.

Step 3 Click **Add** next to Cisco Call Manager (CCM).

Step 4 From the CCM Cluster Details menu, enter the following:

- Software Version—<*UnifiedCMVersion*>, for example, **CCM : 7.1.x**
- Name—<*uniquename*>; for example, **e2c1**
- Description—<*cucmclusterdescript*>; for example, **City 2 cluster 7.1.3**
- Publisher Host Name—<*publisheripaddress*>; for example, **10.131.2.2**
- Publisher Unified CM Name—<*shorthostname*>; for example, **e3c1p**
- Wins Hostname—<*shorthostname*>; for example, **e3c1p**

Note This field is configurable only if the chosen Unified CM version is 4.x.

- Publisher IP Address—<*publisheripaddress*>; for example, **10.131.2.2**
- Publisher Config Username:

- For 4.x—<*4.xpublisherusername*>; for example, **administrator**
- For 5.x—<*5.xpublisherusername*>; for example, **CCMAdministrator**
- for 6.x—<*6.xpublisherusername*>; for example, **administrator**
- for 7.x—<7.xpublisherusername>, for example: **ccmadmin**

- Publisher Config Password—<*publisherpassword*>; for example, **ipcbuemea**
- Country—<*countrywherecucmis*>; for example, **United Kingdom**
- If the Annunciator server on the Publisher is going to be used, click **Annunciator Server**.
- Annunciator Line Capacity—<*numberofAnnunciatorlines*>; for example, **48**
- If the Conference server on the Publisher is going to be used, click **Conference Server**.
- Conference Streams—<*numberofConferenceStreams*>; for example, **128**
- IPPBX lines—<*numberofippbxlines*>; for example, **30000**
- Max. IPPBX lines per device—<MaxIPPBXLinesperDevice>, for example **40**
- If the Media Termination Point on the Publisher is going to be used, check the **Media Termination Point** checkbox.
- If the MOH server on the publisher is going to be used, click **Music Server**.
- Music lines—<*numberofmusiclines*>; for example, **500**
- If the switchboard/console server on the publisher is going to be used, click **Switchboard/Console server**.
- If the TFTP server on the publisher is going to be used, click **TFTP server**.
- CPID—<*cpid*>; for example, **AUTO**
- Cluster ID—<*clusterid*>; for example, **1**
- Check the **Encrypt configuration sessions?** checkbox.

Step 5 Click **Add**.

Step 6 For all 5.x nd 6.x Cisco Unified CM clusters, select the created Cisco Unified CM cluster and modify the following:

- Minimum AXL Interaction Time—**1.2 Seconds** (this throttles AXL requests sent to Cisco Unified CM to 50 requests per minute).

Repeat this procedure for all Cisco Unified CM clusters and publisher servers.

Adding Cisco Unified Communications Manager Subscriber Servers

To define a Cisco Unified CM subscriber server in a cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster to which you want to add subscriber servers and click **Servers**.

Step 3 Click **Add**.

Step 4 From the Server Details menu, enter the following:

- Host Name—<*subscriberhostname*>; for example, **10.131.2.3**
- Wins Hostname—<*shorthostname*>; for example, **e2c1s1**.

Note This field is configurable only if the chosen Unified CM version is 4.x.

- Unified CM Name—<*shorthostname*>; for example, **e2c1p**
- Description—<*subscriberdescript*>; for example, **City 2 cluster 1.7.1.3 Subscriber 1**
- IP Address—<*subscriberipaddress*>; for example, **10.131.2.3**
- If the TFTP server on the subscriber is going to be used, click **TFTP server** and configure the server order to be **2**
- If the MOH server on the subscriber is going to be used, click **Music Server**, and configure the server order to be **2**
- If the Conference server on the Subscriber is going to be used, click **Conference Server**.
- If the Annunciator server on the Subscriber is going to be used, click **Annunciator Server**.
- If the Media Termination Point on the Subscriber is going to be used, click **Media Termination Point**.
- If the attendant console server on the subscriber is going to be used, click **Attendant Console Server**
- If the CTI manager server on the subscriber is going to be used, click **CTI Manager Server**
- If the MGCP on the subscriber is going to be used, click **MGCP Configured**
- If the H.323 on the subscriber is going to be used, click **H.323 Configured**
- If the SCCP on the subscriber is going to be used, click **SCCP Configured**
- If the SIP on the subscriber is going to be used, click **SIP Configured**

Step 5 Click **Submit**.

Repeat this procedure for all subscriber servers in the cluster and for all Cisco Unified CM clusters.

Defining Cisco Unified Communications Manager Groups

To define a Cisco Unified CM phone group in a cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster to which you want to add a Cisco Unified CM phone group.

Step 3 Click **Groups**.

Step 4 Click **Add**.

Step 5 From the Group Details menu, enter the following:

- Group Name—<*phonegroupname*>; for example, **e2PhoneGroupClu1**

- Description—<*phonegroupdesc*>; for example, **Phone Group in City 2 Cluster 1**
- Maximum Streams Supported—<*maxstreams*>; for example, **10000**
- Click **Use for Phones**.

Step 6 From the Select Servers menu, perform the following:

- Choose all servers that are in the list; for example:
  - **e2c1p** (Publisher)
  - **e2c1s1** (Subscriber 1 Local)
- Set the server order for the selected servers; for example:
  - Server Order—**0- e2c1p**
  - Server Order—**1- e2c1s1**

Step 7 Click **Submit**.

Defining a Cisco Unified Communications Manager Trunk Group in a Cluster

To define a Cisco Unified CM Trunk group in a cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster to which you want to add a Cisco Unified CM phone group.

Step 3 Click **Groups**.

Step 4 Click **Add**.

Step 5 From the Group Details menu, enter the following:

- Group Name—<*phonegroupname*>; for example, **e2TrunkGroupClu1**
- Description—<*phonegroupdesc*>; for example, **Trunk Group in City 2 Cluster 1**
- Maximum Streams Supported—<*maxstreams*>; for example, **10000**
- Click **Use for Trunks**.

Step 6 From the Select Servers menu, perform the following:

- Choose all servers that are in the list; for example:
  - **e2c1p** (Publisher)
  - **e2c1s1** (Subscriber 1 Local)
- Set the server order for the selected servers; for example:
  - Server Order—**0- e2c1p**
  - Server Order—**1- e2c1s1**

Step 7 Click **Submit**.

Importing Softkey and Phone Button Templates

To import the softkey template configured on the Unified CM cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Unified CM cluster for which you want to import Softkey Templates.

Step 3 Click **Import/Refresh Items**.

Step 4 Check the **Softkey Templates** check box.

Step 5 Check the **Phone Button Templates** check box.

Step 6 Click **Import/Refresh Items**.

Viewing Softkey/Phone Button Templates

To view the imported Softkey/Phone Button Templates configured on the Unified CM cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Unified CM cluster for which you want to import Softkey Templates.

Step 3 Click **Import/Refresh Items**.

Step 4 Click **Softkey Templates/Phone Button** Templates.

Repeat this for all Unified CM clusters.

Associating Cisco Unified Communications Manager Clusters with Gatekeepers

To associate a Cisco Unified CM cluster with a gatekeeper, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Click **Connectivity** next to one of the Cisco Unified CM clusters you want to associate with the gatekeeper.

Step 3 Click **PBX=>Gatekeeper**.

Step 4 Click **Connect** next to the gatekeeper you want to associate with the Cisco Unified CM cluster.

Repeat this procedure for all Cisco Unified CM clusters.

Note If the gatekeepers are in a cluster, the Cisco Unified CM cluster should be associated with only one of the gatekeepers in the cluster.

Define Cisco Unified Communications Manager Set

In HUCS7.1a deployment, if the Customers have their locations to be provisioned across more than one Cisco Unified Communication Manager (CUCM) clusters, then CUCM set (with all the CUCM clusters to be included in the set) must be defined in USM for each cluster. This is required for Add Customer transaction which provisions the CUCM clusters in the set for customer locations. Follow the steps below to define CUCM sets:

Step 1 Choose **Network > PBX devices.**

Step 2 Click Associated Devices next to Unified CM cluster for which you want to create a set, for example **e2c1p**

Step 3 Click **Add,** to add a new set.

Step 4 From the Details menu, enter the following:-

- Name—<SetName>, for example, Clus1Clus2Set
- Description—<Description>; for example, **CUCM set for Cluster 1 with Cluster 2**
- Transaction Type—<TransType>

Step 5 Select **Add Customer.**

Step 6 Under Available Devices, choose the IPPBX devices which you want to associate; for example, **e2c2p**

Step 7 Click **Submit**.

Note The above steps to define a CUCM set must be repeated for all clusters in the systems, depending on the customers locations provisioning on different clusters and based on the selected hardware group while adding a customer location.

Defining and Configuring DHCP Servers

To define and configure DHCP servers, you must add, load, and synchronize DHCP servers.

Adding DHCP Servers

The DHCP server is defined in USM as an ISC.

To define a DHCP server, perform the following steps:

Procedure

Step 1 Choose **Network > DHCP Servers**.

Step 2 Click **Add**.

Step 3 Click **Add** next to ISC (ISC.org DHCP server).

Step 4 From the Server Details menu, enter the following:

- Host Name—<*uniquename*>; for example, **BVSM-ENT2**
- IP Address—<*bvsmvirtualIP*>; for example, **10.100.92.21**
- Description—<*dhcpserverdescription*>; for example, **City 2 DHCP server on USM**
- Config User Name—**dhcp**
- Config Password—<defaultpassword> (See Note below)
- Path and name of config file—**/data/extdhcp/dhcp/dhcpd-usm.conf**
- Path and name of leases file—**/data/extdhcp/dhcp/dhcpd.leases**
- Version—**ISC: 3.0.X**

Step 5 Click **Add**.

Note The DHCP server password you enter should match with actual password on USM dhcp server. To check this, logon to USM using root account and do the following

- standalone ~ # ssh dhcp@10.100.92.21
- Password: [Enter the dhcp server default password]
- Last login: Mon Apr 26 06:48:49 UTC 2010 from 10.100.92.91 on pts/0
- Last login: Fri Apr 30 08:03:25 2010 from 10.100.92.91
- dhcp@standalone ~ $

If you are unable to SSH to dhcp using the default dhcp password, change the dhcp server password and enter the same on USM page.

Loading and Synchronizing DHCP Servers

To load and synchronize DHCP servers, perform the following steps:

Procedure

Step 1 Choose **Network > DHCP Servers**.

Step 2 Choose a DHCP server you want to load and synchronize.

Step 3 Click **Load**.

Step 4 Return to the DHCP Server manager screen.

Step 5 Click **Synchronize**.

Repeat this procedure for all DHCP servers.

Note When you load a DHCP server, the dhcpd-usm.conf is updated. When you synchronize a DHCP server, the dhcpd.leases file is updated.

Note DHCP servers can also be added as an IOS Device or Technician.

Using TFTP Servers

When Cisco Unified CM publisher and subscriber servers are added, the administrator can indicate whether they have the TFTP server running. If any of the servers in a cluster is selected to act as a TFTP server, that cluster should be shown in the list of TFTP servers. To verify this, go to **Network > TFTP Servers**.

Note For Hosted UCS 7.1(a) testing the TFTP server is selected on Publisher and remote Subscriber servers.

Defining IP Edge Devices

IP edge devices are used to provide location-specific information, such as the IP helper address for the Cisco Unified CM IP phones, and voice and video bandwidth. The IP edge device is defined in USM as a Technician.

To define an IP edge device, perform the following steps:

Procedure

Step 1 Choose **Network > IP Edge Devices**.

Step 2 Click **Add**.

Step 3 Click **Add** next to Technician (a general purpose product).

Step 4 From the Details menu, enter the following:

- Host Name—<*uniquename*>; for example, **e2clu1cus1loc2IPEdge**
- IP Address—<*ipedgeIP*>; for example, **10.181.2.1** (this is the IP helper address for the phones in City 3 - cluster1 customer 1 location 2)
- Email Address: <*email*>; for example, **admin111@cisco.com**
- Voice WAN Bandwidth (Kbps)—<*voicebandwidth*>; for example, **512**
- Video WAN Bandwidth (Kbps)—<*videobandwidth*>; for example, **1024**

Repeat this procedure for all IP edge devices.

Using Music on Hold Servers

When Cisco Unified CM publisher and subscriber servers are added, the administrator can indicate whether they have the music on hold (MOH) server running. If any of the servers in a cluster is selected to act as an MOH server, that cluster should be shown in the list of music servers. To verify this, go to **Network > Music Servers**.

Note For Hosted UCS 7.1(a) testing the MOH server is selected on Publisher and remote Subscriber servers.

Note Music servers can also be added as a Technician.

Using Conference Servers

Note These are optional steps, and are only required for conference calls. Also note that the Unified CM Conference Bridge Software is defined in USM if the 'Conference Server' tick box was selected during the Publisher and/or Subscriber configuration.

The conference server is defined in USM as a Technician.

The Technician product is used to define Non-software conference bridges. Several steps are required to configure a Conference Bridge

Adding Conference Bridges

To add a conference bridge, perform the following steps:

Procedure

Step 1 Choose **Network > Conference Servers**.

Step 2 Click **Add**.

Step 3 Click **Add** next to Technician (a general purpose product).

Step 4 From the Details menu, enter the following:

- Host Name—<*uniquename*>, the same name used to create the conference bridge on Cisco Unified CM; for example, **Clu1HWconfserver**
- IP Address—<*conferenceIP*>, IP address of the conference bridge device or Cisco Unified CM server (for software conference bridges); for example, **10.181.2.65**
- Technician e-mail—<*emailaddress*>

- Conference Streams—<*conferencestreams*>. The common practice is to use the maximum capacity field value from the Cisco Unified CM conference bridge configuration; for example, **32**.

Repeat this procedure for all conference bridges.

Note USM does not add any configuration to the Cisco Unified CM when adding a conference bridge; therefore, it does not matter which type of conference bridge is configured (software, hardware, WS-SVC-CMM, and so on).

Note The conference bridge name configured in USM must match the name used to create the conference bridge on Cisco Unified CM.

Associating Conference Bridges with Cisco Unified CM Clusters

To associate a Cisco Unified CM cluster with the conference bridge, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Click **Connectivity** next to one of the Cisco Unified CM clusters you want to associate with the conference bridge.

Step 3 Click **PBX=>Conference**.

Step 4 Click **Connect** next to the conference bridge you want to associate with the Cisco Unified CM cluster.

Repeat this procedure for all conference bridges and all Cisco Unified CM clusters.

Configuring Transcoder Servers

To configure a transcoder, you must add the transcoder and then associate it with Cisco Unified CM clusters.

Note This is an optional step, and it is required only if transcoding is required; for example, if devices are using different codecs.

Adding Transcoders

To add a transcoder, perform the following steps:

Procedure

Step 1 Choose **Network > Transcoder Servers**.

Step 2 Click **Add**.

Step 3 From the Details menu, enter the following:

- Host Name—<*uniquename*>, the same name used to create the transcoder on Cisco Unified CM; for example, **e2-xcode1**
- IP Address—<*xcodeIP*>, the IP address of the transcoder device; for example, **10.190.2.111**
- Technician e-mail—<*emailaddress*>
- Transcoder Capacity—<*xcodecapacity*>. The common practice is to use the maximum capacity field value from the Cisco Unified CM transcoder configuration; for example, **32**.

Repeat this procedure for all transcoders.

Note USM does not add any configuration to the Cisco Unified CM when adding a transcoder; therefore, it does not matter which type of transcoder is configured.

Note The transcoder name configured in BVSM must match the name used to create the transcoder on Cisco Unified CM.

Associating Transcoders with Cisco Unified CM Clusters

To associate a Cisco Unified CM cluster with the transcoder, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Click **Connectivity** next to one of the Cisco Unified CM clusters you want to associate with the transcoder.

Step 3 Click **PBX=>Transcoder**.

Step 4 Click **Connect** next to the transcoder you want to associate with the Cisco Unified CM cluster.

Repeat this procedure for all transcoders and all Cisco Unified CM clusters.

Adding Cisco PGW-Cisco Unified CM Cluster Hardware Groups

USM uses hardware groups to determine which network components should be provisioned when a customer or location is added for example. At this stage only Cisco PGW-Cisco Unified CM cluster hardware groups are required.

To add a hardware group, perform the following steps:

Procedure

Step 1 Choose **Network > Hardware Groups**.

Step 2 Click **Add**.

Step 3 From the Hardware Group Details menu, enter the following:

- Name—<*uniquename*>; for example, **pgw2-e2c1-hwgrp**
- Description—<*hwgrpdesc*>; for example, **City 2 PGW 2 Unified CM Cluster 1 Hardware Group**
- Limit usage of this hardware group to **Any Action**.

Step 4 Click Next

Step 5 From the Available Transit Switches menu, choose the required Cisco PGW; for example, **PGW-ENT2**.

Step 6 From the Available PBX Systems menu, choose the required Cisco Unified CM cluster; for example, **e2c1**.

Repeat this procedure for all Cisco Unified CM clusters.

Note For USM to provision the correct components, ensure that only one Cisco PGW and one Cisco Unified CM cluster is selected.

Loading the Cisco PGW and Cisco Unified CM Clusters

At this stage, USM provisions the Cisco PGW and Cisco Unified CM clusters for the first time.

Loading the Cisco PGW

To load the Cisco PGW, perform the following steps:

Procedure

Step 1 Choose **Network > Transit Switches.**

Step 2 Choose the Cisco PGW you want to load.

Step 3 Click **Load**.

Note This updates both USM and the Cisco PGW. Verify on the Cisco PGW that the dial plans have been created and configured.

Loading Cisco Unified CM Clusters

To load a Cisco Unified CM cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX Devices**.

Step 2 Choose the Cisco Unified CM cluster you want to load.

Step 3 Click **Load Static Config.**

This procedure updates the Cisco Unified CM.

Note Verify on the Cisco Unified CM cluster that all the components have been created and configured.

Repeat this procedure for all Cisco Unified CM clusters.

Adding Media Resource Groups and Media Resource Group Lists

Media resource management involves working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources so that all Cisco Unified CMs within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and MOH services.

Media resource groups and media resource group lists are added to each Cisco Unified CM cluster.

Adding Media Resource Groups

To define a media resource group in a cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster to which you want to add a media resource group and click **Media Services**.

Step 3 Click **Media Resource Groups**.

Step 4 Click **Add**.

Step 5 From the Details menu, enter the following:

- Name—<*mrgname*>; for example, **e2mrgClu1**
- Description—<*mrgdescript*>; for example, **Media Resource Group in City 2 Cluster 1**

Step 6 From the Group Members menu, choose all available music, conference, and transcoder servers that are in the list.

Step 7 Click **Add**.

This procedure updates both USM and Cisco Unified CM.

Note Verify on the Cisco Unified CM cluster that the media resource group has been created and configured.

Repeat this procedure for all media resource groups and all Cisco Unified CM clusters.

Adding Media Resource Group Lists

To define a media resource group list in a cluster, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster to which you want to add a media resource group list and click **Media Services**.

Step 3 Click **Media Resource Group Lists**.

Step 4 Click **Add**.

Step 5 From the Details menu, enter the following:

- Name—<*mrglname*>; for example, **e2mrglClu1**
- Description—<*mrgldescript*>; for example, **Media Resource Group List in City 2 Cluster 1**

Step 6 From the Select Media Resource Groups menu, choose all available media resource groups that are in the list, in the required order.

Step 7 Click **Add**.

Note When selecting media resource groups to add to the media resource group list, only the media resource groups that are associated with this cluster are displayed.

Note This procedure updates both USM and Cisco Unified CM; it creates the Media resource group list. Verify on the Cisco Unified CM cluster that all the media resource groups have been created and configured.

Repeat this procedure for all media resource group lists and all Cisco Unified CM clusters.

Assigning a Media Resource Group List to Cisco Unified Communications Manager Trunks

To assign a media resource group list to a Cisco Unified CM trunk, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Choose a Cisco Unified CM cluster you want to assign a media resource group list to a trunk.

Step 3 Click **Trunk Config**.

Step 4 Choose the Cisco Unified CM cluster trunk; for example, **e2c1-External**.

Step 5 Click **Modify**.

Note When selecting media resource group lists to assign to the trunk, only the media resource group lists that are associated with this cluster are available.

Note This updates both USM and Cisco Unified CM. Verify on the Cisco Unified CM cluster that the media resource group list is assigned to the Cisco Unified CM trunk.

Repeat this procedure for all Cisco Unified CM clusters.

Conferencing in Hosted UCS

Note If Hosted UCS7.1a is deployed without Hardware Conference Bridge and Transcoder, the CUCM clusters must be configured with following device region associations, for the ad-hoc conference to work using CUCM software conference bridges. The steps mentioned in this sections is to be performed after provisioning HUCS 7.1a deployment

In HUCS7.1a, three-way ad-hoc conferencing is tested with the configuration as follows:

Procedure:

Step 1 Check the Regions of software Conference Bridge and H.225 GK controlled trunk to HSI on CUCM clusters.

Step 2 If there is no association between these two regions, configure the inter-region relationship codec to be G.711. This is because, intra-region codec is G.711 and inter-region codec is G.729 by default on CUCM. Hence, configuring G.711 to be inter-region codec for these two regions enables the conference call to use G.711 and makes it work.

CHAPTER 4

Managing Countries and Provider Resources

This chapter describes how to use USM to define and configure customers and other objects and resources used within the Hosted Unified Communications Services platform. This chapter includes the following sections:

Adding Countries

Note Ensure that all Cisco PGWs and Unified CM clusters are defined at this stage, because it is not possible to add additional Cisco PGWs and Unified CM clusters after a country is added.

This section describes the steps required to add and configure countries. It includes the following topics:

Adding a Country

To add a country, perform the following steps:

Procedure

Step 1 Choose **Provider Administration > Countries**.

Step 2 Click **Add**.

Step 3 Choose the country you want to add; for example, **United Kingdom**.

Step 4 Click **Add**.

This procedure updates USM, the Cisco PGW, and Unified CM. Verify on the Cisco PGW and on all Unified CM clusters that all the components have been created and configured.

Note Verify on the PGW and on all Unified CM clusters that all the components have been created and configured.

Editing the Incoming Cisco PGW Trunk Group

As part of Hosted UCS 7.1(a) static configuration, for the interface between the Cisco PGW and PSTN, a per-country route list to PSTN was created: rtlist2pstn<*Country_code*>. For example, *rtlist2pstn44* for the United Kingdom.

This route list is associated to one or more routes, which in turn are associated with a number of trunk groups. For these trunk groups, the custgrpid property can now be updated with the correct country specific P#PADDEDDCC# dial plan:

```
prov-ed:trnkgrpprop:name="<rttrnkgrp_name>",custgrpid="P#PADDEDDCC#", for example:
prov-ed:trnkgrpprop:name="2001",custgrpid="P044",
```

Following is a sample mml session for a redundant Cisco PGW pair:

```
prov-sta::srcver="active",dstver="P044dp"
prov-ed:trnkgrpprop:name="2001",custgrpid="P044"
prov-dply
```

Creating an Inventory of E.164 Numbers, IP Addresses, and Phones

This section describes the steps required to create an inventory or E.164 numbers, IP addresses, and phones at the provider level. This inventory is later assigned to resellers, customers, customer divisions, and finally customer locations.

This section includes the following topics:

- Creating an E.164 Inventory, page 4-2
- Creating an IP Address Inventory, page 4-3
- Creating a Phone Inventory, page 4-4

Creating an E.164 Inventory

To create an inventory of E.164 numbers, you must first define area codes and then add a range of numbers for the specific area code. Together, they give a range of E.164 numbers that are later assigned to customer locations.

Adding Area Codes

To add an area code, perform the following steps:

Procedure

Step 1 Choose **Resources > E.164 Inventory**.

Step 2 Choose a country to which you want to add an area code and click **Next**.

Step 3 Click **Area Code Mgt**.

Step 4 Click **Add**.

Step 5 From the Enter Area Code menu, enter National Area Code—<*areacode*>; for example, **1402**.

Step 6 Click **Add**.

Repeat this procedure for all area codes.

Adding Number Ranges

To add a number range, perform the following steps:

Procedure

Step 1 Choose **Resources > E164 Inventory**.

Step 2 Choose a country to which you want to add a number range and click **Next**.

Step 3 Enter a National Area Code—<*areacode*>; for example, **1402**, and click **Next**.

Step 4 Click **Add Number Range**.

Step 5 From the Details menu, enter the following:

- Start of number range—<*startofnumberrange*>; for example, **111000**
- End of number range—<*endofnumberrange*>; for example, **111019**

Step 6 Click **Add**.

Repeat this procedure for all required number ranges and for all area codes.

Creating an IP Address Inventory

To create an inventory of IP addresses, you define an IP subnet that is associated with a DHCP server, IP edge device, DNS server, and so on. The IP subnet is later assigned to customer locations.

To add an IP subnet, perform the following steps:

Procedure

Step 1 Choose **Resources > IP Address Inventory**.

Step 2 Click **Add**.

Step 3 From the Details menu, enter the following:

- IP Subnet—<*ipsubnet*>; for example, **10.181.2.0**
- Subnet Mask—<*subnetmask*>; for example, **/26**
- DHCP server controlling this subnet—<*dhcpserver*>; for example, **BVSM-ENT2**
- IP edge device to which this subnet is connected—<*ipedge*>; for example, **e2clu1cus1loc1IPEdge**
- Origin IP of DHCP messages encapsulated by router—<*defaultip*>; for example, **10.181.2.1**
- DHCP helper IP address—<*bvsmvirtualIP*>; for example, **10.100.92.21**
- Backup DHCP helper IP address—<*bvsmvirtualIP*>; for example, **10.100.92.21**
- Domain Name—<*domainname*>; for example, **ipcbuemea.cisco.com**
- Primary DNS server IP—<*primaryDNS*>; for example, **10.100.201.10**
- Fallback DNS server IP—<*fallbackDNS*>; for example, **10.100.202.10**
- IP address for default route of phone—<*defaultrouteIP*>; for example, **10.181.2.1**

Step 4 Click **Add**.

Repeat this procedure for all IP subnets.

Creating a Phone Inventory

Inventory of IP phones is first created at the provider level. The IP phones can later be assigned to resellers, customers, customer divisions, or customer locations.

To add an IP phone, perform the following steps:

Procedure

Step 1 Choose **Resources > Phone Inventory**.

Step 2 Click **Add**.

Step 3 From the Details menu, enter the following:

- Enter the MAC address of the phone—<*macaddress*>; for example, **0018192945EA**
- From the drop-down menu, choose the phone type; for example, **Cisco 7961 SIP**.
- Button Template Name—Use the default template for phone type

Note By default, a phone type is associated to a default phone button template, which is defined during the initial basic setup.

Step 4 Click **Add Phone**.

Repeat this procedure for all phones.

Adding Resellers

Resources defined at the provider level (line types, phone types, and service types) can be assigned to the reseller at this stage.

To create a reseller, perform the following steps:

Procedure

Step 1 Choose **General Administration > Resellers**.

Step 2 Click **Add**.

Ensure that you are adding a reseller for the correct provider. The name of the provider is shown on the screen, as shown in Figure 4-1:

Figure 4-1 Adding Resellers—Provider Level (UKProvider)

Step 3 From the Details menu, add the following:

- Name—<*ResellerName*>; for example, **UKReseller1**
- Country—<*Country*>; for example, **UK**
- Post/Zip Code—<*Post/Zip Code*>
- Contact Name—<*ContactName*>
- Contact Telephone Number—<*ContactTelephoneNumber*>

Step 4 From the Line Types menu, add the required number of lines for each line type; for example, **2000**.

Step 5 From the Phone Types menu, add the required number of phones for each phone type; for example, **2000**.

Step 6 From the Service Types menu, add the required number of subscribers for each service; for example, **2000**.

Step 7 From the GUI Branding menu, define the type of branding for the User Interface.

To define default branding, select **Default GUI branding** and click **Default GUI branding**.

Step 8 Click **Add**.

Repeat this procedure for all required resellers.

Managing Customers

This section describes the required steps to define customers, customer resources (for example media services), and feature groups. Resources defined at the reseller level (line types, phone types, and service types) can be assigned to the customer at this stage.

The administrator will define the dialing prefix used for calls between customer locations if this option was enabled when the dial plan was created.

Feature groups define the class of service to be allocated to a user or a phone. Feature groups are created at the customer level and are common across all locations within that customer.

This section includes the following topics:

- Adding Customers, page 4-6
- Adding Media Services, page 4-7
- Adding Feature Groups, page 4-8
- Configuring USM User Roaming Preferences

Adding Customers

To create a customer, perform the following steps:

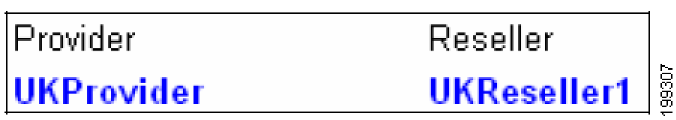
Procedure

Step 1 Choose **General Administration > Customers**.

Step 2 Click **Add**.

Ensure that you are adding a customers for the correct reseller. The name of the reseller is shown on the screen, as shown in Figure 4-2.

Figure 4-2 Adding Customers—Reseller Level (UKReseller1)



Step 3 From the Details menu, add the following:

- Name—<*CustomerName*>; for example, **UKCustomer1**
- Country—<*Country*>; for example, **UK**
- Post/Zip Code—<*Post/Zip Code*>
- Contact Name—<*ContactName*>
- Contact Telephone Number—<*ContactTelephoneNumber*>

Step 4 From the Corporate Directory Details menu, add the IP Address—<*BVSMvirtualIP*>; for example, **10.100.92.21**.

Step 5 From the Enter Number of Lines Required menu, add the required number of lines for each line type; for example, **500**.

Step 6 From the Enter Number of Phones Required menu, add the required number of phones for each phone type; for example, **500**.

Step 7 From the Enter Subscriber Numbers for each Service menu, add the required number of subscribers for each service; for example, **500**.

Step 8 From the Dial Plan Details menu, do the following:

- Add the Default Hardware group—<*cushwgrp*>; for example, **e2pgwcucmhwgrpclu1**.

- Add the Inter-Site Prefix—<*intersiteprefix*>; for example, **8**.
- Click **Automatically Generate Site codes**.

Step 9 From the Please Select Required Themes menu, do the following:

- Add the Default branding of User Interface—**Default GUI branding**.
- Click **Default GUI branding**.

Step 10 Click **Add**.

This procedure updates both USM and Cisco PGW.

To verify the values of the of the variables: #CUSTDIALPLAN#, #EGRESSCUSTDIALPLAN#, #EGRESSCUSTDIALPLAN2# , #COMMONLEGACYPBX#, #INGRESSLEGACYPBX#, #EGRESSLEGACYPBX#, #VOICEMAILDIALPLAN#, perform the following steps:

Procedure

Step 1 Choose **General Administration > Customers**.

Step 2 Choose a customer.

Step 3 Click **AdvancedMgt**.

Step 4 Click **View PGW Config**.

Step 5 Choose the relevant Cisco PGW; for example, **PGW-ENT2**.

Note Verify on the Cisco PGW that the dial plans have been created and configured.

Repeat this procedure for all required customers.

Adding Media Services

USM does not assign media resource group lists directly to a location. USM uses a resource called media services, which can be assigned to a location. To use a media resource group list on a location, a media service must be added that contains the media resource group list.

The media service can contain three components: a conference server, an MOH server, and/or a media resource group list.

Note The conference server and MOH server fields in the media service are used for non-Unified CM resources. When adding the media service, choose only the media resource group list.

To add a media service, perform the following steps:

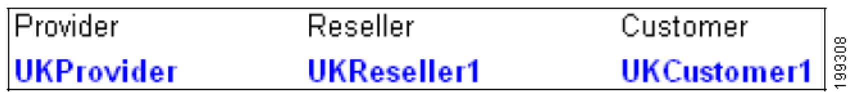
Procedure

Step 1 Choose **Resources > Media Services**.

Step 2 Click **Add**.

Ensure that you are adding media services for the correct customer. The name of the customer is shown on the screen, as shown in Figure 4-3.

Figure 4-3 Adding Media Services—Customer Level (UKCustomer1)



Step 3 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **e2msClu1Cus1**
- Description—<*mediaservicedesc*>; for example, **City 2 Media Service (MRGL) Cluster 1 Customer 1**

Step 4 From the Select Media Groups menu, add the Name—<*mrglname*>; for example, **e3mrglClu1**.

Step 5 Click **Add**.

Repeat this procedure for all required Unified CM clusters, and for all required customers.

Adding Feature Groups

Feature groups define the class of service to be allocated to a user or a phone. Feature groups are created at the customer level and are common across all locations within that customer.

To add a feature group, perform the following steps:

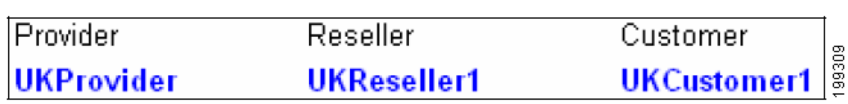
Procedure

Step 1 Choose **General Administration > Feature Groups**.

Step 2 Click **Add**.

Ensure that you are adding a feature group for the correct customer. The name of the customer is shown on the screen, as shown in Figure 4-4.

Figure 4-4 Adding Feature Groups—Customer Level (UKCustomer1)



Step 3 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **COS1International24Hour**
- Description—<*featuregroupdesc*>; for example, **COS1International24Hour**

- Outbound Calls Limitations—<*outbound*>; for example, **COS1International24Hour**
- Call Forward Limitations—<*callforwardlim*>; for example, **COS1CF**
- VoiceMail Profile—<*voicemailprofile*>; for example, **Basic VoiceMail profile**
- Inbound Call options—<*inbound*>; for example, **Allow one DDI line**
- Number of Ext or Lines—<*ExtorLinesNumber*>; for example, **One Number DDI or Extension**
- Tick all fields that are relevant for the Unified CM release on which the Feature Group is to be applied.

Step 4 Click **Submit**.

Repeat this procedure for all required features, and for all customers.

Configuring USM User Roaming Preferences

If the USM UserRoaming preference setting has been enabled at the provider level, the following two additional preferences can be configured at the Customer level:

- **AllowCrossClusterLogin**—for a user with Extension Mobility, this setting enables users to log into phones away from their home Unified CM Cluster, by using the Cross Cluster Forwarding feature.
- **ForceOldRoamingLogoff—**for a user with Extension Mobility, this setting forces the user to be logged out from the old phone if he logs in to another phone.

To configure these settings, perform the following steps:

Step 1 Go to **General Administration > Customers**. Select a Customer for which you want to activate the feature

Step 2 Click **Preferences**.

Step 3 Click **AllowCrossClusterLogin**.

Step 4 Check the available checkbox to enable the setting.

Step 5 Click **Modify**.

Step 6 Click **Return to Preferences Management**.

Step 7 Click **ForceOldRoamingLogoff**

Step 8 Tick the available box to enable the setting.

Step 9 Click **Modify**.

Repeat this procedure for all required customers.

Tip Ensure that **User Mobility** and **Allow User login to Phone** are selected in the feature group to be used by the user.

Adding Divisions

This section describes the steps required to create a customer division. Resources defined at the customer level (line types, phone types, and service types) can be assigned to the customer division at this stage.

To create a customer division, perform the following steps:

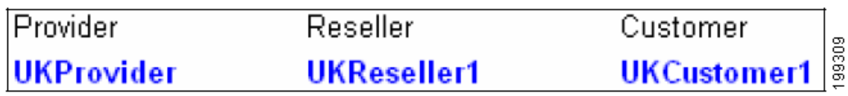
Procedure

Step 1 Choose **General Administration > Divisions**.

Step 2 Click **Add**.

Ensure that you are adding a division for the correct customer. The name of the customer is shown on the screen, as shown in Figure 4-5.

Figure 4-5 Adding Divisions—Customer Level (UKCustomer1)



Step 3 From the Details menu, add the following:

- Name—<*DivisionName*>; for example, **UKDivision1**
- Address—<*Address*>
- City—<*City*>
- Country—<*Country*>; for example, **UK**
- Post/Zip Code—<*Post/ZipCode*>
- Contact Name—<*ContactName*>
- Contact Telephone Number—<*ContactTelephoneNumber*>

Step 4 From the Line Types menu, add the required number of lines for each line type; for example, **500**.

Step 5 From the Phone Types menu, add the required number of phones for each phone type; for example, **500**.

Step 6 From the Service Types menu, add the required number of subscribers for each service; for example, **500**.

Step 7 From the Please Select Required Themes menu, enter the default branding of User Interface—**Default GUI branding**.

Step 8 Click **Default GUI branding**.

Step 9 Click **Add**.

Repeat this procedure for all required divisions.

Adding Locations

This section describes the required steps to define customer locations. Resources defined at the customer division level (line types, phone types, and service types) can be assigned to the customer locations at this stage. You define which Hosted UCS network components are associated with the location by selecting an appropriate hardware group. The following are also selected:

- Location site code
- Length of the phone extensions (if this option was enabled when the dial plan was created)
- Dialing prefix used to make calls to the PSTN (if this option was enabled when the dial plan was created)
- Default area code
- IP subnet for the location

Caution If the location requires Enhanced Emergency Support (Cisco Emergency Responder (Cisco ER) is used to route Emergency Calls), ensure that the relevant Cisco ER Group is connected to the Unified CM cluster where the location will be provisioned.

To create a location, perform the following steps:

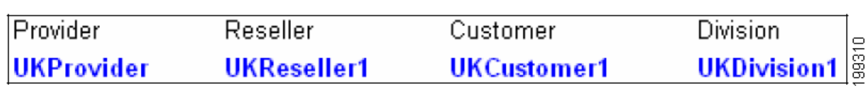
Procedure

Step 1 Choose **General Administration > Locations**.

Step 2 Click **Add**.

Ensure that you are adding a location for the correct customer division. The name of the reseller is shown on the screen, as shown in Figure 4-6.

Figure 4-6 Adding Locations - USM administrator at the Division level - UKDivision1



Step 3 From the Details menu, add the following:

- Location Name—<*LocationName*>; for example, **1402clu1cus1loc1**
- Address—<*Address*>
- City—<*City*>
- Country—<*Country*>; for example, **UK**
- TimeZone—<*Area/Location*>; for example, **Europe/London**
- Post/Zip Code—<*Post/Zip Code*>
- Contact Name—<*ContactName*>
- Hardware Group—<*lochwgrp*>; for example, **e2pgwcucmhwgrpclu1**
- PBX Template—Default.

Note For Hosted UCS 7.1(a) the Default value should be used, so that different locations can be configured using different Unified CM models

- Enhanced Emergency Support—<*EnhEmergSupport*>; select this option if Cisco ER is used to route Emergency Calls

Note If you select Enhanced Emergency Support, the location gets provisioned with two translation patterns (911 and 9.911) which are used to detect emergency calls and route them to Cisco ER.

- Single Number Reach Support—select this option if SNR feature support is required for this location.

Step 4 From the Dial Plan menu, add the following:

- Site Code—<*LocSiteCode*>; for example, **111**
- Dial this to get an outside line—<*PSTNacce*> *ssprefix*>; for example, **9**
- Select extension number length—<*ExtLength*>; for example, 3
- Default Area Code—<*DefAreaCode*>; for example, **1402**
- Local Dialing—You can select seven-digit local dialing, ten-digit local dialing, or no local dialing; for example, **7-digit**

Note Local Dialing is only available while adding Locations in the US.

Step 5 From the Subnets menu, enter the IP subnet assigned to Location <*LocSubnet*>; for example, **10.181.2.0/26.**

Step 6 From the Please Select Required Themes menu, do the following:

- Add the Default branding of User Interface—Default GUI branding.
- Click **Default GUI branding**.

Step 7 Click **Next >>**.

Step 8 From the Line Number menu, enter the required number of lines for each line type; for example, **20**.

Step 9 From the Services menu, enter the required number of subscribers for each service; for example, **20**.

Step 10 Click **Next >>**.

Step 11 From the Phone Types menu, enter the required number of phones for each phone type; for example, **20**.

Step 12 Click **Add**.

This procedure updates, USM, Cisco PGW, and Unified CM.

To verify the location-specific Unified CM configuration, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Telephony**.

Step 2 Choose a location.

Step 3 Click **Telephony**.

Step 4 Click **Advanced Diagnostics**.

Step 5 Choose the relevant Unified CM cluster; for example, **e2c1**.

Note Verify on the Cisco PGW that the dial plans have been created and configured, and on the Unified CM cluster that the partitions, CSSs, route patterns, and translation patterns have been added.

Repeat this procedure for all required locations.

Moving Inventory of E.164 Numbers and Phones to Locations

This section describes the steps required to move the inventory of E.164 numbers and phones created at the provider level to the customer locations.

Note IP addresses (IP subnets) created at the provider level are automatically associated with locations when the locations are created.

Ensure that you are moving the inventory of E.164 numbers and phones to locations at the correct provider level. To get to the provider level, choose **Provider Administration > Providers** and choose a provider.

The name of the provider appears on the screen.

This section includes the following topics:

- Moving E.164 Number Inventory, page 4-13
- Moving Phone Inventory, page 4-14

Moving E.164 Number Inventory

To move a range of E.164 numbers to a location, perform the following steps:

Procedure

Step 1 Choose **Resources > E.164 Inventory**.

Step 2 Choose a country to which you want to add a number range.

Step 3 Click **Next**.

Step 4 Choose a value for National Area Code—<*areacode*>; for example, **1631**.

Step 5 Click **Next**.

Step 6 Click **Move Number Range**.

Step 7 From the Details menu, enter the following:

- Select Location—<*requiredlocation*>; for example, **UKReseller1: UKCustomer1: UKDivision1: 1402clu1cus1loc1**

- Start of number range—<*startofnumberrange*>; for example, **14021111000**
- End of number range—<*endofnumberrange*>; for example, **1102111019**

Step 8 Click **Move**.

Repeat this procedure for all required locations.

Moving Phone Inventory

To move a phone to a location, perform the following steps:

Procedure

Step 1 Choose **Resources > Phone Inventory**.

Step 2 Choose the phone you want to move to a location by clicking the MAC address of the phone; for example, **001D452CDA84**.

Step 3 Click **Next**.

Step 4 Choose a Move Target—<*requiredlocation*>; for example, **UKReseller1: UKCustomer1: UKDivision1: 1402clu1cus1loc1**

Step 5 Click **Next**.

Step 6 Choose a value for Subnet—<*locationsubnet*>; for example, **10.181.2.0**.

Step 7 Click **Move Phone**.

This procedure updates both USM and Unified CM.

Note The phone and a line are added to the Unified CM, and the phone registers with the Unified CM, but the phone has very restrictive settings. In USM, the phone appears as unregistered.

Repeat this procedure for all required phones and for all required locations.

Administering Locations

This section describes the steps required to do the following:

- Configure various location-specific parameters (for example, the PSTN published number, emergency published number, and so on)
- Assign a range of E.164 numbers to internal numbers
- Register and manage phones (for example, reset a phone, modify phone properties, and so on)
- Add and manage end users
- Add extension mobility

Ensure that you are administering the correct location. The name of the location appears on the screen.

This section includes the following topics:

Adding PSTN Published Numbers

If the PSTN published number is configured, when a call from an IP phone is destined to the PSTN (basic or call forwarded), the calling party number (CgPN) and the redirecting number are replaced with the PSTN published number if the phone does not have an associated E.164 number.

To add a PSTN published number, perform the following steps:

Procedure

Step 1 Choose **General Administration > Locations**.

Step 2 Choose a location to which you want to add the PSTN published number and click **Advanced Mgt**.

Step 3 Click **PSTN Published Number**.

Step 4 From the Details menu, enter the following:

- Published PSTN Number—<*PSTNPubNumber*>; for example, **1402111009**

Step 5 Click **Add**.

This procedure updates both USM and Cisco PGW.

Repeat this procedure for all required locations.

Adding Emergency Published Numbers

The emergency published number is required to correctly route emergency calls. After the emergency published number is configured, when an emergency call is placed, the CgPN is replaced with the emergency published number.

To add an emergency published number, perform the following steps:

Procedure

Step 1 Choose **General Administration > Locations**.

Step 2 Choose a location to which you want to add the emergency published number.

Step 3 Click **Advanced Mgt**.

Step 4 Click **Emergency Number**.

Step 5 For Emergency Number—<*EmPubNum*>, select an available E.164 number; for example, **1402111008**.

Step 6 Click **Add**.

This procedure updates both USM and Cisco PGW.

Repeat this procedure for all required locations.

Assigning Range of E.164 Numbers to Internal Numbers

If the location requires PSTN calls to be routed via Local PSTN breakout, instead of proceeding with the provisioning step in this section ensure that

- Location preference AssociateFNNinRanges is enabled;
- Location is connected to the relevant Local Gateway Interface
- Range of E.164 numbers is assigned to a range of Internal numbers in ranges

To enable the flag FwdRedirectingExternalNumonCallFwd at provider level, do the following:

Step 1 Navigate to provider level for example, **UKProvider1**.

Step 2 Click **Advanced Mgt**.

Step 3 Click **Advanced Telephony Settings**.

Step 4 Check the **FwdRedirectingExternalNumonCallFwd** check box.

Step 5 Click **Apply.**

For a range of internal extensions, the USM administrator can assign a range of E.164 numbers. Thesecan then be assigned to an IP Phone, so that users can receive calls from the PSTN on those extensions

Assigning Range of E.164 Numbers to Internal Numbers (in-ranges)

To assign a range of E.164 numbers to internal numbers using the in-ranges option, perform the following steps:

Procedure

Step 1 Choose **Location Administration > External Numbers**.

Step 2 Click **Associate Range**.

Step 3 From the Details menu, enter the following for the range:

- PSTN Number range—<*PSTNRange*>; for example, **1402111000-1402111009**
- Extension Number range—<*ExtRange*>; for example, **000-019**

Step 4 Click **Submit**.

Note Starting from Hosted UCS 6.1(a) USM invokes the PGW TimesTen driver and uses the TimesTen Input in the AssociateFNN transaction (AssociateFNN script) of the PGW_TimesTen model worksheet to create an import file and transfer it to the PGW, where it invokes the HUCSprovx10 PGW script and inserts the associations into the PGW TimesTen database.

Registering Phones

To register a phone, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Phone Registration**.

Step 2 Choose the phone you want to register by clicking the MAC address of the phone; for example, **001D452CDA84**.

Step 3 From the Phone Features menu, enter the following:

- Phone Location—<*PhoneLocation*>; for example, **Phone Switch 04 -Port1**
- Softkey Template—<*SoftkeyTemplate*>; for example, **Softkey_Advanced**
- Button Template Name—<PhoneButtonTemplate>; for example, **Standard 7975 SCCP**
- First Expansion Module—<None>
- First Expansion Module—<None>
- Select Phone Feature Group—<PhoneFeatureGroup>, for example COS1International24Hour
- Click Next >>

Step 4 From the Number Details menu, enter the following:

- Line Number—<*ExtOrE164*>; for example, **DDI 1402111001**
- Label—<*PhoneLabel*>; for example, **SCCP 001**
- Line Class of Service—Select **COS1International24Hour**

Note If required and possible, you can add multiple lines.

Step 5 Click **Register**.

This procedure updates both USM and Unified CM.

Repeat this procedure for all required phones, and for all required locations.

Adding an End User

To add an end user, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Users**.

Step 2 Click **Add**.

Step 3 From the Details menu, enter the following:

- Username—<*Username*>; for example, **clu1cus1loc1user1**

Note From HUCS7.1a onwards, the end user name must not exceed 15 characters. This is the limitation on the USM on the length of end user name.

- Password—<*Password*>; for example, **cisco123**
- Role—<*Role*>; for example, **End User for clu1cus1loc1**
- First Name—<*FirstName*>
- Last Name—<*LastName*>

Step 4 Click **Next >>**.

Step 5 From the Details menu, enter the following:

- Phone PIN—<*PhonePIN*>, minimum 5 digits; for example, **12345**
- Feature Group—<*UserFeatureGroup*>; for example, **COS1International24Hour**
- Access Profile—Default

Step 6 Click **Add**.

This procedure updates both USM and Unified CM.

Repeat this procedure for all required users and for all required locations.

Adding User Extension Mobility

Extension mobility can be set up to enable users to login to phones on their home Unified CM cluster.

To add extension mobility for a user, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Users**.

Step 2 Click **Add** next to the user to which you want to add extension mobility.

Step 3 From the User Mobility Profile menu, enter the following:

- Phone Type—<*UserPhoneType*>; for example, **Cisco 7961 SCCP**
- Button Template Name—<*UserButtonTemplate*>; for example, **Standard 7961 SCCP**

- Softkey Template—<*UserSoftkeyTemplate*>; for example, **Softkey_Advanced**

Step 4 From the Number Details menu, enter the following:

- Select the Extension from the drop-down menu—<*ExtOrE164*>; for example, **DDI 1402111002**
- Label—<*PhoneLabel*>; for example, **user1**
- Line Class of Service: <LineCOS>; for example, **COS1International24Hour**

Step 5 Click **Add**.

Note If required and possible, you can add multiple lines.

This procedure updates both USM and Unified CM.

Repeat this procedure for all required users, and for all required locations.

Managing Phones

To manage a phone, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Phone Management**.

Step 2 Choose the user you want to manage by clicking the username; for example, **001D452CDA84**.

You can use this page to do the following:

- Reset the phone
- Login a user
- Logout a user
- Modify the phone button template
- Modify the phone locale
- Delete lines
- Modify phone features; for example, enable or disable PC support, enable or disable speaker, and so on
- Modify line settings; for example, enable or disable hot line, enable or disable call forwarding, and so on
- Unregister the phone

This procedure updates both USM and Unified CM.

Managing Users

To manage a user, perform the following steps:

Procedure

Step 1 Choose **Location Administration > Users**.

Step 2 Choose the phone you want to manage by clicking the MAC address of the phone; for example, **cus1loc1user1**.

You can use this page to do the following:

- Change the user password
- Change the user PIN
- Modify or delete user extension mobility
- Associate the user to a phone
- Delete the user

This procedure updates both USM and Unified CM.

CHAPTER 5

Managing Legacy PBX Support

Legacy PBX support lets the Hosted Unified Communications Services platform environment support call flows to and from PBXs and for the required Cisco PGW configuration to be provisioned by USM. Media gateways can be connected to PBXs using PRI Q.931, PRI QSIG, or DPNSS, and the signalling is reliably backhauled via the media gateway to the Cisco PGW. Various ISR and non-ISR routers are supported.

This chapter includes the following sections:

Defining IOS Devices

In the Hosted UCS environment for legacy PBX support, BVSM needs the information about what type of media gateways are connected to the PBX to provision the Cisco PGW. The BVSM administrator defines an IOS device (type, network modules, and interface cards). This information is later used to add and configure the media gateways.

Ensure that you are adding IOS device components to the correct provider. To get to the provider level, choose **Provider Administration > Providers** and choose a provider.

The name of the provider appears on the screen.

Adding IOS Device Types

To add an IOS device type, perform the following steps:

Procedure

Step 1 Choose **Setup Tools > Vendor Tools**.

Step 2 Click **Add**.

Step 3 Click **Add** for Transit Connected MGCP Legacy PBX Gateway .

Step 4 From the Details menu, enter the following:

- Host Name—<Host name of the IOS Device>; for example, **e2qsig**
- Description—<IOSDeviceTypeDesc>; for example, **City2 QSIG legacy PBX gateway**
- Country—Select <Country>; for example, **United Kingdom**
- Owner—Select <Provider>; for example, **UKprovider**
- Uncheck Single Location Only check box **C3845**.

Note If you enable Single Location Only, the IOS device can be used in the selected location only. Single Legacy PBX gateway ports can be allocated to different unmanaged locations which require PBX support. Hence, unselect Single Location Only check box.

Step 5 Under Connectivity Details, enter the following:

- IP Address—<EthInterface IP Address>; for example, **10.190.2.40**
- IP Address (alternate): <Alternate IP Address>; for example, **10.191.2.40**
- IP Domain—<Domain name>; for example, **ipcbuemea.cisco.com**

Note Domain name should be same as hostname of the IOS device. This is due to USM issue in which only domain name is taken to create PGW switch trunk MGCP endpoint, which does not match with gateway MGCP endpoint name. Hence, gateway MGCP registration fails

- Config Password—Enter <IOS device config password>; for example, **cisco**
- Enable Password—Enter <IOS device enable password>; for example, **cisco**

Step 6 Click **Finish.**

Repeat this procedure for all IOS device types.

Adding Gateway

To add a Media Gateway, do the following:

Procedure

Step 1 Choose **Network > IOS Devices**.

Step 2 Click the IOS Device; for example, **e2qsig.**

Step 3 From Device Roles menu, click **Add on Gateway**.

Step 4 From the Gateway Details menu, enter the following:

- Name—<GW hostname>; for example, **e2qsig**
- Description—<GW description>; for example, **City2 QSIG legacy PBX gateway**
- Select Protocol—for example **MGCP**
- Click **Next**.
- Select Device— <Transit Switch: PGW-ENT2 version 9.7.3>

Note In Hosted UCS 7.1(a), PGW 9.8(1) is also supported apart from PGW 9.6.1 and 9.7.3.

Step 5 Click **Next.**

Step 6 From the Gateway Functions menu, ensure **Legacy** is enabled for location

Step 7 Click **Add**.

Repeat this procedure for all IOS device network modules.

Add and Configure Ports

To add and configure gateway ports:

Step 1 Choose **Network > IOS Devices**.

Step 2 Click the IOS Device, for example **e2qsig**.

Step 3 Click the Gateway under Gateway Details, for example **e2qsig**.

Step 4 Click the **Gateway Hardware Configuration,** under Interface Details.

Step 5 From Legacy Ports menu, click Add Port and enter the following:

- Port Type—Select <PortType>; for example, **E1**
- Port Number—<Slot/SubUnit/Port>; for example, **1/0/0**

Note If the E1 port configured on the Gateway has 2-tuple (ex. 1/0), then some times the Channel ID mismatch happens as the DCHAN configured on the PGW side is set to 3-tuple value by default. Hence, make sure that the E1 port configuration should have 3-tuple value (ex. 1/0/0) "Slot/subunit/port" when you face issues with the following PGW signaling services are not in service.
IPFASPATH and **DCHAN** for qsig/q931 backhaul signalling.

- Port Description—<Description>; for example **E1 Port on e2qsig**

Step 6 Click **Add**.

Step 7 Click Configure on the added port under Legacy Ports, enter the following:

- Port Description—<Description>; for example, **E1 Port on e2qsig**
- Under Port Configuration, Framing—Select <Framing>; for example, **Non CRC4**
- Clock Source—for example, **Line**

- Line Coding—<line Coding type>; for example, **HDB3**
- ISDN Switch Type—Select <SwitchType>; for example, **primary-qsig**
- ISDN Side—Select <SwitchSide>; for example, **Network**

Note Hosted UCS side is always meant to be network side by default.

Step 8 Click **Add.**

Repeat this for all Gateway ports configuration

Using Unmanaged PBX Devices

This section describes how PBXs are defined in USM. The PBX is created as an unmanaged PBX. This unmanaged PBX device is only used as a parent component for the location. It also describes how to create a hardware group that contains only the unmanaged PBX and the Cisco PGW that is used to connect to the PBX gateway. No Unified CM clusters should be added to this hardware group.

Ensure that you are adding unmanaged PBXs and the Cisco PGW unmanaged PBX hardware groups to the correct provider. To get to the provider level, choose **Provider Administration > Providers** and choose a provider.

Adding Unmanaged PBXs

To define an unmanaged PBX, perform the following steps:

Procedure

Step 1 Choose **Network > PBX devices**.

Step 2 Click **Add**.

Step 3 Click **Add** next to UnmanagedPBX (Unmanaged PBX).

Step 4 From the Details menu, enter the following:

- Host Name—<*uniquename*>; for example, **cus1unmqsigpbx1**
- Description—<*UnmanagedPBXesc*>; for example, **Customer 1 Unmanaged QSIG PBX 1**
- Country—<*CountrywherePBXis*>; for example, **United Kingdom**
- E-mail Address—<*emailaddress*>

Step 5 Click **Add**.

Note Hostname of the unmanaged PBX device must be unique across all device types available in USM.

Repeat this procedure for all required unmanaged PBXs.

Adding a Cisco PGW Unmanaged PBX Hardware Group

To add a hardware group, perform the following steps:

Procedure

Step 1 Choose **Network > Hardware Groups**.

Step 2 Click **Add**.

Step 3 From the Hardware Group Details menu, enter the following:

- Name—<*uniquename*>; for example, **pgw2-e2qsig-hwgrp**
- Description—<*hwgrpdesc*>; for example, **City 2 "Unmanaged QSIG PBX - PGW" Hardware**
- **Group Customer 1**
- Limit usage of this Hardware Group to—**Any Action**

Step 4 From the Available Transit Switches menu, choose the required Cisco PGW; for example, **PGW-ENT2**.

Step 5 From the Available PBX Systems menu, choose the required unmanaged PBX; for example, **cus1unmqsigpbx1**.

Repeat this procedure for all unmanaged PBXs.

Note Ensure that only one Cisco PGW and one unmanaged PBX is selected, for USM to provision the correct components.

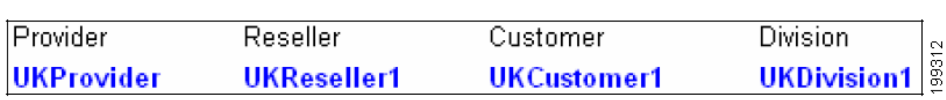
Adding Unmanaged PBX Locations

Note If you did not create a customer division, customer, or reseller for the unmanaged PBX location, go back and complete steps described in Adding Resellers, page 4-5, Managing Customers, page 4-5, or Adding Divisions, page 4-10, before proceeding.

The PGW-Unmanaged PBX hardware group is used when an unmanaged PBX location is added. This ensures that BVSM provisions only the Cisco PGW during the AddLocation transaction. The unmanaged PBX location is used only to move/associate E.164 numbers to the PBX.

Ensure that you are adding unmanaged PBX locations for the correct customer division. The name of the reseller is shown on the screen, as shown in Figure 5-1.

Figure 5-1 Adding Unmanaged PBX Locations—Division Level (UKDivision1)



To create an unmanaged PBX location, perform the following steps:

Procedure

Step 1 Choose **General Administration > Locations**.

Step 2 Click **Add**.

Step 3 From the Details menu, add the following:

- Location Name—<*LocationName*>; for example, **unmqsigpbxcus1loc1**
- Address—<*Address*>
- City—<*City*>
- Country—<*Country*>; for example, **UK**
- TimeZone—<*Area/Location*>; for example, **Europe/Londo**n
- Post/Zip Code—<*Post/Zip Code*>
- Contact Name—<*ContactName*>
- Location Type—<TypeofLocation>, Select Unmanaged Location

Step 4 Click **Next >>**.

Step 5 From the Details menu, add the following:

- Hardware Group—<unmpbxlocochwgrp>; for example, **pgw2-e2qsig-hwgrp**
- PBX Template—Default

Step 6 From the Dial Plan menu, add the following:

- Site Code—<*LocSiteCode*>; for example, **131**
- Dial this to get an outside line—<*PSTNaccessprefix*>; for example, **9**
- Select extension number length—<*ExtLength*>; for example, **3**
- Default Area Code—<*DefAreaCode*>; for example, **1402**

Step 7 From the Please Select Required Themes menu, add the following:

- Default branding of User Interface—**Default GUI branding**
- Click **Default GUI branding**.

Step 8 Click **Next >>**.

Step 9 From the Line Number menu, enter the required number of lines for internal extensions; for example, **50**.

Step 10 Click **Add**.

Repeat this procedure for all required locations.

Creating an E.164 Inventory

To create an inventory of E.164 numbers for unmanaged PBX locations, the administrator first needs to define area codes, and then add a range of numbers for the specific area code. Together, they give a range of E.164 numbers that are later assigned to unmanaged PBX locations.

Add Area Codes

To add an Area Code, do the following:

Step 1 Choose **Resources > E164 Inventory.**

Step 2 Select a Country for which you want to add an Area Code.

Step 3 Click **Next.**

Step 4 Click **Area Code Mgt.**

Step 5 Click **Add.**

Step 6 From Enter Area Code menu, enter the following

- National Area Code—<areacode>; for example, **1631**

Step 7 Click **Add.**

Repeat this for all Area Codes.

Add Number Range

To add a Number Range, do the following:

Step 1 Choose **Resources > E164 Inventory.**

Step 2 Select a Country for which you want to add a Number Range.

Step 3 Click **Next.**

Step 4 Select National Area Code—<areacode>, for example **1631.**

Step 5 Click **Next**.

Step 6 Click **Add Number Range**.

Step 7 Under Details, enter the following:

- Start of number Range: <startofnumberrange>; for example, **131000**
- End of number Range: <endofnumberrange>; for example, **131019**

Step 8 Click **Add**.

Repeat this for all required number ranges and for all area codes.

Move E.164 Number Inventory

To move a range of E.164 Numbers to an Unmanaged PBX Location:

Step 1 Choose **Resources > E164 Inventory.**

Step 2 Select a Country for which you want to move the Number Range.

Step 3 Click **Next.**

Step 4 Select National Area Code—<areacode>; for example, **1631.**

Step 5 Click **Next.**

Step 6 Click Move Number Range.

Step 7 Under Details, enter the following:

- Select Location—<requiredlocation>; for example, **UKReseller1 : UKCustomer1 : UKDivision1 : unmqsigpbxcus1loc1**
- Start of number Range—<startofnumberrange>; for example, **1631131000**
- End of number Range—<endofnumberrange>; for example, **1631131019**

Step 8 Click Move.

Repeat this for all required unmanaged PBX locations

Adding PSTN Published Numbers

After the PSTN published number is configured, when a call from a legacy PBX phone is destined to the PSTN via the central gateway (basic or call forwarded), the CgPN and the redirecting number are replaced with the PSTN published number.

To add a PSTN published number, see Adding PSTN Published Numbers, page 4-15.

Adding Emergency Published Numbers

The emergency published number is required to correctly route emergency calls. After the emergency published number is configured, when an emergency calls is placed, the CgPN is replaced with the emergency published number. For the procedure, see Adding Emergency Published Numbers, page 4-15.

This procedure updates both USM and Cisco PGW.

Repeat this procedure for all required unmanaged PBX locations.

Assigning Range of E.164 Numbers to Internal Numbers

For a range of internal extensions, the USM administrator can assign a range of E.164 numbers. These can then be assigned to a legacy PBX phone, so that users can make calls to the PSTN from those extensions.

For the procedure, see Assigning Range of E.164 Numbers to Internal Numbers, page 4-16. This procedure updates both USM and Cisco PGW.

Note From Hosted UCS 6.1(a), USM invokes the PGW TimesTen driver and uses the TimesTen Input in the AssocaiteFNN transaction (AssociateFNN-UnmanagedPBX script) of the PGW_TimesTen_Any model worksheet to create an import file and transfer it to the PGW, where it invokes the HUCSprovx10 PGW script and inserts the associations into the PGW TimesTen database.

Repeat this procedure for all required unmanaged PBX locations.

Configure Media Gateway and PGW

To configure IOS media gateway and PGW for PBX support, the administrator needs to:

- Allocate Gateway Port to Unmanaged Location
- Activate Legacy Gateway

Allocate Gateway Port to Unmanaged Location

To allocate ports, do the following:

Step 1 Choose **Network > IOS Devices.**

Step 2 Click the IOS Device, for example **e2qsig.**

Step 3 Click the Gateway under Gateway Details, for example **e2qsig**.

Step 4 Under the legacy interfaces section on the IOS Gateway main page, Click **Port Allocation.**

Step 5 Under the legacy Port Allocation section Unallocated Ports, on the **IOS Gateway main page**

- Select Location—The unmanaged PBX location; for example, **unmqsigpbxcus1loc1**
- Allocate—Check the check box on the port to allocation; for example, **1/0/0**

Step 6 Click Allocate

Repeat this for all required Media Gateways.

Activate Legacy Gateway

Note Activating legacy gateway interface for PBX support requires both master and slave PGW IP address details. Hence, ensure that both master and slave PGW details are available in USM for the PGW under **Network > Transit Switches**.

In Hosted UCS 7.1(a), the gateway port activation provisions the gateway and PGW for legacy PBX support. To activate the port do the following:

Step 1 Navigate to the Unmanaged location, for example **unmqsigpbxcus1loc1**

Step 2 Choose **Location Administration > Telephony > Legacy Gateways.**

Step 3 Under Location Details, enter the following

- Select **MGCP** as the Gateway Protocol.
- Click **Next >>**
- Call Limit—<Call limit>; for example, **31**

Step 4 Under Location Trunk Details, enter the following:

Default DN—<LocationDefaultDN>; for example, **131001**

Own Routing Number—<RoutingNumber>; for example, **131001** (For DPNSS only)

Step 5 Under Legacy Interface details, enter the following:

- Tick the interface to be activated under Available Interfaces
- Enter the Priority—<TrunkpriorityonPGW>; for example 1

Step 6 Click Submit.

Repeat this for all required Gateway interfaces to be activated.

Note After a Gateway or E1 has been provisioned into the PGW, USM does not put the associated functions into service. Similarly with deleting, USM does not take the required functions out of service which will allow the E1 or Gateway to be removed from the PGW. The service state must be manipulated manually on the PGW.

Verify QSIG signalling backhaul service status on PGW

Note Signalling service name or links may vary depending on the signalling protocol. Below steps are applicable to QSIG/Q931 signalling protocols only.

After provisioning E1 port, do the following on PGW to ensure QSIG backhaul signalling services are up:

Step 1 Set the IP signalling links into In Service (IS) state. On the PGW MML prompt, select USM provisioned IP links and set their state to IS.

- PGW-ENT2 mml > set-iplnk:iplnk1-X:IS
- PGW-ENT2 mml > set-iplnk:iplnk2-X:IS

Where 'X' is the Gateway ID which can be obtained from USM "Gateway Hardware Configuration" page for that media gateway.

Step 2 Ensure that following Q931 back haul signalling services are up on the PGW.

a. To check IPFAS signalling link, use the following mml command on PGW:

- PGW-ENT2 mml > rtrv-dest:ipfas-XY:

Where X is the Gateway ID and Y is E1 port ID (Slot/SubUnit/Port). For example,

- PGW-ENT2M mml> rtrv-dest:ipfas-8100:
- MGC-01 - Media Gateway Controller 2010-07-08 10:20:37.370 BST
- M RTRV

```
"ipfas-8100:PKG=ISDNPRI,ASSOC=SWITCHED,PST=IS,SST=RSTO"
;
```

- PST=IS indicates that the IPFAS signalling link is In Service

b. To check Dchannel status, use the following mml command on PGW

- PGW-ENT2 mml > rtrv-dchan:dchan-XY:

Where X is the Gateway ID and Y is E1 port ID (Slot/SubUnit/Port). For example,

- PGW-ENT2M mml> rtrv-dchan:dchan-8100:
- MGC-01 - Media Gateway Controller 2010-07-08 10:29:08.060 BST
- M RTRV

```
"dchan-8100:ipfas-8100,LID=0:IS"
/* Dchannel-8100 */
;
```

- LID=0:IS indicates that PRI Dchannel is In Service.

When removing legacy gateway configuration, the following commands are required to be done on PGW before removing gateway E1 trunk configuration:

```
set-iplnk:iplnk1-X:OOS
set-iplnk:iplnk2-X:OOS
set-iproute:ipr-X:OOS
set-dest:ipfas-XY:OOS
```

Where X is the Gateway ID and Y is E1 port ID (Slot/SubUnit/Port).

CHAPTER 6

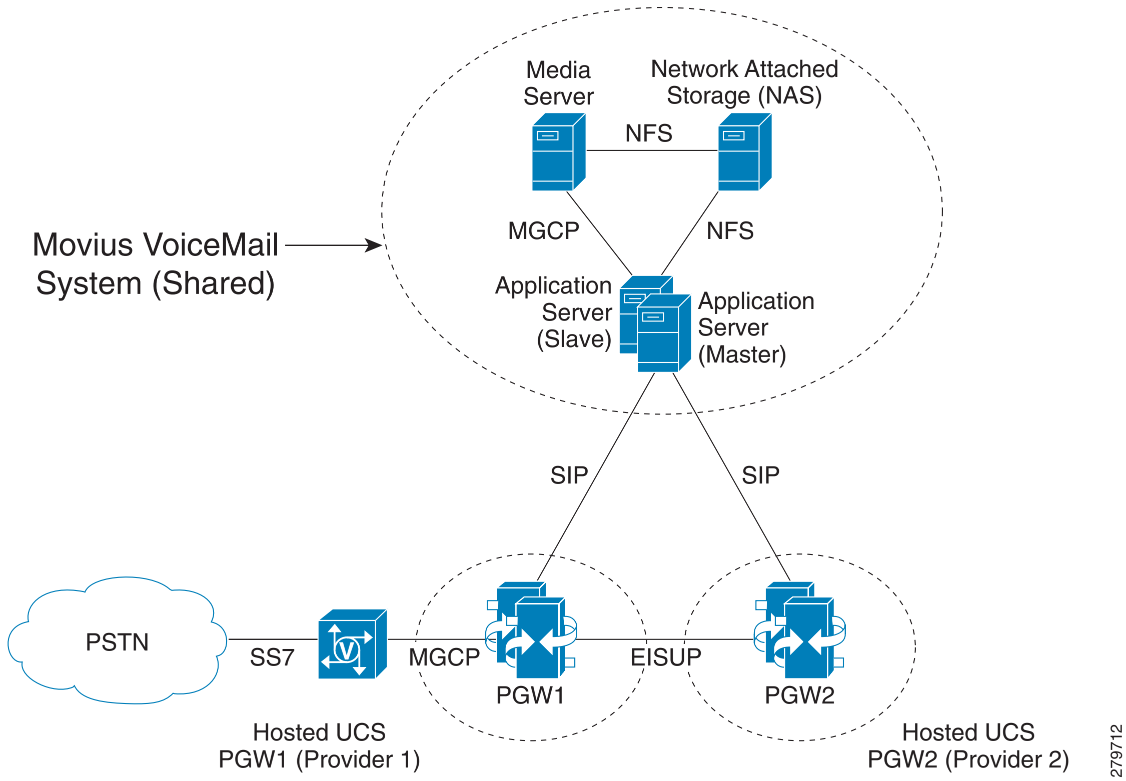
Provisioning Movius VoiceMail and Auto Attendant Services

This chapter describes the provisioning of Movius VoiceMail and Auto Attendant services and configuring SBC for the Movius Auto Attendant to work with PGW. Also, it contains the configuration details needed in PGW and Movius. This chapter includes the following sections:

Provisioning Movius IP Unity Voicemail support

This section describes the provisioning of Movius VoiceMail support for multiple Hosted UCS platforms using one Movius VoiceMail system. The figure below shows the Movius VoiceMail System Integration into Hosted UCS.

Figure 6-1 Movius VoiceMail System Integration into Hosted UCS



A typical Movius VoiceMail System comprises the following:

- Application server – The Application Server is a SUN Netra Server with a Solaris operating system where the Voice Mail State Machine is running. The State Machine is responsible for handling all phone calls coming into the system (for Hosted UCS the application server communicates with the PGW). The Application Server also hosts the database that stores all subscriber and application-related data. The Application Server also controls the Media Server. The Application Server can be run as a redundant pair (Master/Slave).
- Media Server - The Media Server is the custom hardware that terminates all media. It provides services, such as announcements, digit collection, and message recording. The Mereon Application Server controls the Media Server. The Media Server terminates the media stream.
- Network Attached Storage – The Network Attached Storage (NAS) stores all voice and fax message files. The application server, media server, and proxy server have access to the NAS using NFS.

This section describes the following topics:

- Static Configuration, page 6-3
- Loading the Movius Model, page 6-9
- Defining and Configuring Movius VoiceMail Network Elements, page 6-10
- Movius VoiceMail Customer Administration, page 6-14
- Movius VoiceMail Location Administration, page 6-18

Static Configuration

This topic details the initial static (manual) configuration required for Movius VoiceMail support of the following HUCS components:

- CUCM Static Configuration, page 6-3
- Cisco PGW StaticConfiguration, page 6-3
- Movius 4.2 Static Configuration, page 6-5

CUCM Static Configuration

To enable CUCM to support voice mail Message Waiting Indication (MWI) from Movius IP Unity, the following CUCM service parameters are to be updated:

- Set “Multiple Tenant MWI Modes” to true. It enables CUCM to use translation patterns to convert voice-message mailbox numbers into directory numbers when your voice-messaging system issues a command to set a message waiting indicator
- Ensure that, “Message Waiting Indicator Inbound Calling Search Space” set to <None>.

Cisco PGW StaticConfiguration

To enable the PGW to communicate with the Movius VoiceMail System, the following SIP components need to be provisioned on the PGW:

SIP Automatic Switchover Using Dual-VLAN - The following XECfgParm.dat parameters need to be configured on both Active and Standby PGW:

```
*.Virtual_IP_Addr1 = <VirtualIPAddress1>   # Must be from *.IP_Addr1 Subnet.
*.Virtual_IP_Addr2 = <VirtualIPAddress2>   # Must be from *.IP_Addr2 Subnet.
*.sipFailover   = true     # Failover if SIP Service fails.
```

for example

```
*.Virtual_IP_Addr1 = 10.120.2.13   # Must be from *.IP_Addr1 Subnet.
*.Virtual_IP_Addr2 = 10.121.2.13   # Must be from *.IP_Addr2 Subnet.
*.sipFailover   = true     # Failover if SIP Service fails.
```

Note For further details refer to http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/feature/module/9.4_1_/FMvlan.html

SIP Signaling Service - The SIP signaling service is the connection between the PGW and a SIP server. To add a SIP signaling service:

```
prov-add:sippath:name="<sip-sigpath>",mdo="IETF_SIP",desc="<Description>"
```

For example:

```
prov-add:sippath:name="Moviussippath",mdo="IETF_SIP",desc="SIP signaling service
Movius-PGW"
```

SIP Signaling Link. The SIP signaling link is the connection between the PGW and the SIP server. To add a SIP signaling link:

```
prov-add:siplnk:name="<sip-sipchan>",ipaddr="Virtual_IP_Addr1",svc="<sip-sigpath>",port=50
60,pri=1,desc="<Description>",
```

for example:

```
prov-add:siplnk:name="Moviussiplnk-1",port=5060,pri=1,svc="Moviussippath",ipaddr="Virtual_
IP_Addr1",desc="siplnk1 Movius-Pgw"
```

```
prov-add:siplnk:name="Moviussiplnk-2",port=5060,pri=2,svc="Moviussippath",ipaddr="Virtual_
IP_Addr2",desc="siplnk2 Movius-Pgw"
```

SIP Trunk Group for incoming SIP calls from Movius to PGW. To add a SIP trunk group:

```
prov-add:trnkgrp:name="<trnkgrp_name>", svc="<sip-sigpath>",type="SIP_IN",
```

for example:

```
prov-add:trnkgrp:name="3001",svc="Moviussippath",type="SIP_IN"
```

SIP Trunk Group Properties of the previously created SIP Trunk Group for incoming SIP calls from Movius to PGW. To configure SIP trunk group properties, the SIP profile should be added and linked to trunk group:

```
prov-add: profile:
name="<profile_name>",type="SIPPROFILE",custgrpid="<custgrpid>",mgcdomain="<MGC_Domain>",
mgcsipversion="<SIP_Version>",localport="<Local_Port>", Support183="3"
prov-add: trnkgrpprof:name="<trnkgrp_name>",profile="<profile_name>",
```

for example:

```
prov-add:
profile:name="moviusippf-3001",type="SIPPROFILE",custgrpid="ICCM",mgcdomain="pgw-ent2",mgc
sipversion="SIP/2.0",localport="5060",Support183="3"
prov-add:trnkgrpprof:name="3001",profile="moviusippf-3001"
```

Note The MGCDomain indicates the PGW domain name used in SIP messages. On Movius this value should be used in the "/etc/hosts" file to resolve the PGW IP Addresses.

Note Enter the ICCM dial plan for the incoming calls from Movius to the PGW.

SIP Trunk Group for outgoing SIP calls from PGW to Movius - To add a SIP trunk group:

```
prov-add:trnkgrp:name="<trnkgrp_name>", svc="<sip-sigpath>",type="IP_SIP",
```

for example:

```
prov-add:trnkgrp:name="3002",svc="Moviussippath",type="IP_SIP"
```

SIP Trunk Group Properties of the previously created SIP Trunk Group for outgoing SIP calls from PGW to Movius - To configure SIP trunk group properties, the SIP profile should be added and linked to trunk group:

```
prov-add: profile:
name="<profile_name>",type="SIPPROFILE",custgrpid="<custgrpid>",mgcdomain="<MGC_Domain>",
mgcsipversion="<SIP_Version>",localport="<Local_Port>",
Support183="3",unsolicitednotifymethod="1”
prov-add: trnkgrpprof:name="<trnkgrp_name>",profile="<profile_name>",
```

for example:

```
prov-add:profile:name="moviussippf-3002",type="SIPPROFILE",
custgrpid="ICCM",mgcdomain="pgw-ent2",MGCsipversion="SIP/2.0",localport="5060",support183=
"3",unsolicitednotifymethod="1"
prov-add:trnkgrpprof:name="3002",profile="moviussippf-3002"
```

Note UnsolicitedNotifyMethod="1" is required in order to enable the "Unsolicited NOTIFY" method for unsolicited notification of SIP DTMF digits by PGW.

SIP Routing Trunk Group Properties of the previously created SIP Trunk Group for outgoing SIP calls from PGW to Movius - To add the SIP routing trunk group properties:

```
prov-add:siprttrnkgrp:name="<trnkgrp_name>",srvrr=0,cutthrough=2,version="2.0",extsupport=
1,sipproxyport=5060,
url="<SES _Virtual_IP>",
```

for example:

```
prov-add:siprttrnkgrp:name="3002",srvrr=0,cutthrough=2,version="2.0",extsupport=1,sipproxy
port=5060,url="10.100.91.31"
```

Note The URL is configured with the Secure Execution Server (SES) Virtual IP address of the Movius Application Servers.

Route to Movius - To add the route:

```
prov-add:rttrnk:name="<rttrnk_name>",trnkgrpnum=<rttrnkgrp_name>,weightedTG="OFF",
```

for example:

```
prov-add:rttrnk:name="rte2movius",trnkgrpnum=3002,weightedtg="OFF"
```

Route List to Movius - To add the route list:

```
prov-add:rtlist:name="<rtlist_name>",trnkgrpnum=<rttrnk_name>,weightedTG="OFF",
```

for example:

```
prov-add:rtlist:name="rtlist2ipunity",rtname="rte2movius",distrib="OFF"
```

Tip Calls from the PGW to Movius are routed from the "EGRV" dial plan using the rtlist2ipunity route list.

Repeat these PGW provisioning steps for each Hosted UCS Platform.

Below is an example extract from the config.mml for the PGW in City 2:

```
prov-add:sippath:name="Moviussippath",mdo="IETF_SIP",desc="SIP signaling service
Movius-PGW"
prov-add:siplnk:name=
"Moviussiplnk-1",port=5060,pri=1,svc="Moviussippath",ipaddr="Virtual_IP_Addr1",desc="sipln
k1 Movius-Pgw"
prov-add:siplnk:name=
"Moviussiplnk-2",port=5060,pri=2,svc="Moviussippath",ipaddr="Virtual_IP_Addr2",desc="sipln
k2 Movius-Pgw"
prov-add:trnkgrp:name="3001",svc="Moviussippath",type="SIP_IN"
prov-add:trnkgrpprop:name="3001",custgrpid="ICCM",MGCDomain="pgw-ent5",MGCSipVersion="SIP/
2.0",LocalPort="5060",Support183="3"
prov-add:trnkgrp:name="3002",svc="Moviussippath",type="IP_SIP"
prov-add:
profile:name="moviusippf-3001",type="SIPPROFILE",custgrpid="ICCM",mgcdomain="pgw-ent2",mgc
sipversion="SIP/2.0",localport="5060",Support183="3"
prov-add:trnkgrpprof:name="3001",profile="moviusippf-3001"
prov-add:profile:name="moviussippf-3002",type="SIPPROFILE",
custgrpid="ICCM",mgcdomain="pgw-ent2",MGCsipversion="SIP/2.0",localport="5060",support183=
"3",unsolicitednotifymethod="1"
prov-add:trnkgrpprof:name="3002",profile="moviussippf-3002"
prov-add:
siprttrnkgrp:name="3002",srvrr=0,cutthrough=2,version="2.0",extsupport=1,sipproxyport=5060
, url="10.100.91.31"
prov-add:rttrnk:name="rte2movius",trnkgrpnum=3002,weightedtg="OFF"
prov-add:rtlist:name="rtlist2ipunity",distrib="OFF",rtname="rte2movius"
```

Note For detailed information, refer to the Cisco Media Gateway Controller Software Release 9 Provisioning Guide.

Movius 4.2 Static Configuration

Movius Application servers also need some static (manual) configuration. This topic explains the following:

Defining PGWs on the Movius system

Log into the Movius system configuration page.

Note The system configuration page can be accessed via: http://<IP_Unity_GUI_IP_Address>/sysconfig/webconfig/login-javascript.jsp

Step 1 Enter the following in the system configuration page:

- NAT IP—**10.78.97.70** (Internal IP: 10.100.91.72)
- Username—**system**
- Password—**ipunity**

Note After logging in, the PGWs for each Hosted UCS platform that uses the Movius VoiceMail system should be configured. The PGWs are defined in Movius as SIP Call Agents.

Step 2 Go to **Call Agent > SIP Call Agent and** Click **Add.**

Step 3 In the **SIP Call Agent**, enter the following:

- Name—<pgw_name>, for example **PGW-ENT5**
- Host Name/IP Address—<MGCDomain>, for example **pgw-ent5** (This should be the same value as the PGW SIP Trunk Group property "MGCDomain")
- Call Agent type—**Cisco BTS10200 4.4**

Step 4 Click **Save**.

The first configured SIP Call Agent (PGW) should be set as the Default MWI and Outgoing Call Agent Type. To configure this follow the following steps:

Step 1 Go to **Call Agent**.

Step 2 Enter the following in the **MWI Agent Properties**:

- Default MWI Call Agent type—<first_pgw_name>, for example **SIP**
- Default MWI Call Agent—**PGW-ENT5**

Step 3 Enter the following in the **Please Select a default Call Agent**:

- Default Outgoing Call Agent—<first_pgw_name>, for example **PGW-ENT5**

- Click **Update**.

Mapping the PGW IP Addresses to Host Names

The Host Name (PGW SIP Trunk Group property “MGCDomain”) configured for the Movius Application server SIP Call Agent, should also be mapped to the SIP Virtual IP Addresses of the redundant PGWs.

For example, City 5 PGWs are configured with the following:

```
################################################################
# Improved SIP Failover Support. Setting 0.0.0.0 to both will disable
# the SIP Improved failover support Feature. Configuring only one will
# cause the switchover, if the physical interface where it present fails.
#
*.Virtual_IP_Addr1 =                10.120.5.13   # Must be from *.IP_Addr1 Subnet.
*.Virtual_IP_Addr2 =                10.121.5.13   # Must be from *.IP_Addr2 Subnet.
################################################################
```

On the Movius Application Server (active and standby), the mapping should be configured in the “/etc/hosts” file. Following is an example of the configured “hosts” file for two PGW redundant pairs:

```
IPCBU-UM3A:root@/$ cd /etc
IPCBU-UM3A:root@/etc$ more hosts
############################################
### Virtual SIP IP Addresses of pgw-ent5 ###
############################################
10.120.5.13     pgw-ent5
10.121.5.13     pgw-ent5
```

Enabling Centrex Support

Centrex is the name of the feature, which supports partitioning on Soft switches. Centrex allows different partitions to support their own private numbering plans so that subscribers in those partitions can dial each other using short extension numbers rather than long public numbers.

Movius UM server supports Centrex by way of organizations and public and private telephone numbers. Organizations are analogous to partitions on the soft switch while private telephone numbers are analogous to the extensions on the soft-switch.

In Movius UM server organizations are identified with orgId which has one-to-one mapping with “centrex-id” or “bgid” on the soft-switch. To map organization created on the Movius UM server to a business (or Centrex) group on the soft-switch, each organization can be provisioned with “Centrex-Id” or “bgid”

Note This field will be visible on the configuration page for organization only if system is enabled for Centrex.

Once Centrex is enabled on the Movius UM server, whenever any telephone number is added in the system (either pilot number or subscriber phone number), administrator will have a choice of specifying that number as public or private. Public telephone numbers are unique in the system. Private telephone numbers on the other hand are unique only within the same organization (or partition). So for example, two organizations A and B can have the same private telephone number 1000 without any conflict. Private telephone numbers are always resolved with the help of accompanying Centrex-Id (or bgid).

Note Any telephone number added before enabling Centrex, is provisioned as public telephone number.

To enable Centrex support do the following:

Step 1 Go to **System > Voice Mail >Voice mail from Web Settings**.

Step 2 Click **Edit**.

Step 3 Check the Centrex Enabled box.

Step 4 Click **Update.**

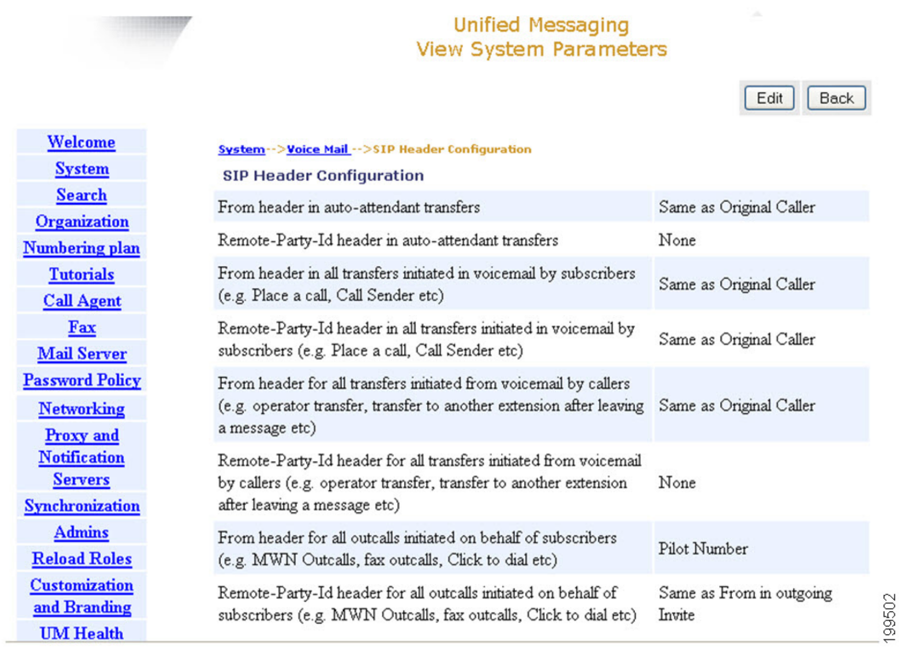
Changing SIP Header on Movius

Following changes need to be made on IP Unity system , so that it sends the A number of calling party instead of AA pilot number.

Step 1 Navigate to **System >Voicemail > SIP Header Configuration**.

Step 2 Set the parameters for SIP Header as shown in the figure 6-2.

Figure 6-2 Movius UM Configuration - SIP Header Configuration



Changing SIP Mandatory Headers on the database

In HUCS7.1a, the PGW makes a delayed offer call to the Movius on the SIP trunk, whereas Movius expected early offer (expecting SDP in the invite message). To change the behavior of Movius to accept the delayed offer, following commands are to be executed on the Movius4.2 system.

Logon to Movius UM application server using SSH and enter the following commands:

```
movius-um1-app-2:root@/$ sesdb
SQL*Plus: Release 10.1.0.2.0 - Production on Wed Jun 9 16:04:01 2010
```

```
Copyright (c) 1982, 2004, Oracle.  All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - 64bit Production
With the Partitioning, OLAP and Data Mining options
SQL> update MANDATORY_HEADER_CHECK set MANDATORYHEADERS='Call-Id,Startline,From,
To,Via,Contact,CSeq'  where MESSAGE='REQ:INVITE' and DIRECTION='INCOMING';
SQL> update frameconfig set value='false' where property = 'sendInitialRemoteSdp';
SQL> commit;
```

Restart framework process on all application nodes using the following command:

```
ipunityctl restart fw
```

Disabling Numbering Dial Plan on Movius

In order to make calls from the Auto Attendant, we need to disable the Numbering Dial Plan.

Procdeure

Step 1 Log to each node of the Movius cluster by SSH.

Step 2 Go to Tools folder— **/opt/ipunity/tools** and run the script **setSysParamInDB.ksh.** and give the argument **"bypassNumPlanCheck true"**.
root@/opt/ipunity/tools$ ./setSysParamInDB.ksh bypassNumPlanCheck true

```
SQL*Plus: Release 10.1.0.2.0 - Production on Fri Aug 22 04:36:16 2008
Copyright (c) 1982, 2004, Oracle.  All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - 64bit Production
With the Partitioning, OLAP and Data Mining options
SQL>
1 row deleted.
SQL>
1 row created.

SQL>
Commit complete.

SQL> Disconnected from Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP and Data Mining options
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
crane >> System parameters reloaded.
crane >> Connection to localhost closed by foreign host.
```

Loading the Movius Model

In Movius UM version 4.2.1.3, the values in the "webPasswordPolicyName" and the "tuiPasswordPolicyName" fields in the IPUnity worksheet of the model have to match the configured Password Policy names on the Movius UM system configuration. To verify the configured names, log into Movius UM system configuration and click Password Policy. By default, the "webPasswordPolicyName" is def_web_passwdpol2, and the "tuiPasswordPolicyName" is def_tui_passwd_pol2. If you do not want to configure different Email and TUI Password Policies, change the following lines in the IPUnity_Any worksheet:

```
HUCS AddVMServicePilot <webPasswordPolicyName>def_web_passwdpol2</webPasswordPolicyName>
HUCS AddVMServicePilot <tuiPasswordPolicyName>def_tui_passwd_pol2</tuiPasswordPolicyName>
```

Also ensure that the column where the centrexId is configured in not commented out:

```
HUCS AddVMServicePilot <centrixId>#CENTREXID#</centrixId>
```

Prepare USM by loading the Movius Model.

Procedure

Step 1 Go to **Dialplan Tools > Configuration Models**.

Step 2 Browse for the model loader being used and click **Submit**.

Note NOTE: Check for any errors or warnings at the completion of loading.

Defining and Configuring Movius VoiceMail Network Elements

This section describes required steps to define and configure Movius VoiceMail network elements. It also shows how the components are associated to each other and describes how the PGWs and Cisco Unified CMs are configured for Movius VoiceMail support.

Defining Movius VoiceMail Server

Movius VoiceMail server is defined in USM as an ‘Movius Server’.

Procedure:

Step 1 Go to **Network > VoiceMail Servers** and click **Add**.

Or
Go to **Network > IVR** and click **Add.**

Step 2 Click **Add** coresponding to IP Unity Voice Mail Server.

Step 3 Enter the following details in the **Manage IPUnity page**:

- Host Name—<uniquename>, for example **MoviusforCity5**
- IP Addres—<VirtualATJIP>, for example **10.100.91.72**
- Description—<Moviusdescription>, for example **Movius Server for City** 5
- Config User Name—for example, **system**
- Config Password—<configpassword>, for example **ipunity**
- Software Version—for example, **IPUnity : Any**
- Maximum Lines Supported**—**<maxlinesup>, for example:**80000**
- CPID—**<**VoiceMailCPID**>,** for example **AUTO**
- Roles—Check both IVR Server check box and VoiceMail Server check box if both Movius Auto Attendant and Voicemail are required. If not, check just the VoiceMail Server check box.

Step 4 Click **Add**.

Note USM doesn't allow provisioning the same Movius Server with the same IP Address under different providers. As a workaround, an additional Virtual IP address for Apache on the Movius UM servers is created for the additional provider.

Note To avoid possible conflicts when creating Movius Organizations, the Movius CPID should be unique across all providers.

Following steps are required to create an additional Virtual IP Address for Apache:

Step 1 Log into the master UM server, for example: **IPCBU-UM3A**

Step 2 Go to **/etc/upsuite: cd /etc/upsuite**

Step 3 Edit the upsuite.conf file, to add an additional Virtual IP Address for Apache. For the new IP Address, following new parameters are required:

- New Service Name—for example, **PRISSCAP31_1** (should be unique),
- New Service ID—for example, **3111**
- New Service IP—for example, **10.100.91.132** (additional Virtual IP Address)
- New Interface—for example, **eri0:62** (same network – ERI0)

Following is an example of the upsuite.conf file (the configuration for the old and new Virtual ATJ IP Address is only shown):

```
<SERVICE NAME="PRISSCAP31" SERVICE_ID="3101" TYPE="BASIC">
<SERVICE_IP IP="10.100.91.32" IF="eri0:61" ROUTE_ADD="FALSE"/>
<NODE_REF NODE_ID="1"/>
<NODE_REF NODE_ID="2"/>
<SPLIT_RES STRATEGY="LOWEST_NODE_ID"/>
<LINK NETWORK="Heartbeat_Network" ROUTE="ROUTE"/>
</SERVICE>
<SERVICE NAME="PRISSCAP31_1" SERVICE_ID="3111" TYPE="BASIC">
<SERVICE_IP IP="10.100.91.132" IF="eri0:62" ROUTE_ADD="FALSE"/>
<NODE_REF NODE_ID="1"/>
<NODE_REF NODE_ID="2"/>
<SPLIT_RES STRATEGY="LOWEST_NODE_ID"/>
<LINK NETWORK="Heartbeat_Network" ROUTE="ROUTE"/>
</SERVICE>
```

Step 4 Once this is done, restart the Movius application, Oracle, and Upbeat:

```
/etc/rc3.d/S98ipunity stop
/etc/rc3.d/S45oracle stop
/etc/rc3.d/S91upbeat stop
/etc/rc3.d/S91upbeat start
/etc/rc3.d/S45oracle start
/etc/rc3.d/S98ipunity start
```

Step 5 Repeat steps 1-4 on the slave UM server, for example: **IPCBU-UM3B**.
The Movius VoiceMail Server can be defined on the second provider using the second Virtual ATJ IP Address.

Creating PGW-Movius VoiceMail Server Hardware Group

USM uses Hardware Groups to determine which Network Components should be provisioned when a customer or location is added. For example, to add the PGW-Movius VoiceMail Server Hardware Group do the following:

Step 1 Go to **Network > Hardware Groups**, and Click **Add**.

Step 2 Enter the following in the **Hardware Group Details**:

- Name—<uniquename>, for example **e3pgwipuhwrgrpclu2**
- Description—<hwgrpdesc>, for example **City 2 PGW-Movius Hardware Group Cluster1**
- Limit usage of this Hardware Group to—**Any Action**

Step 3 In the **Available Transit Switches**, choose the PGW Movius VoiceMail System will connect to, for example **PGW-ENT2**.

Step 4 In the **Available PBX Systems**, choose the Unified CM Cluster used by the Customer, for example **e2c1**.

Step 5 In the **Available VoiceMail Systems**, choose the previously defined Movius server, for example: **MoviusforCity2**.

Step 6 In the **Available IVR Servers**, choose the previously defined Movius server, for example: **MoviusforCity2**.

Step 7 Click **Add**

Note The IVR Server must be selected as part of hardware group, if you plan to have the same Voicemail system to support Auto Attendant.

Associating Movius IVR Server with PGW

This is only required if you are using Movius AA. To associate the Movius IVR System with the PGW do the following:

Step 1 Go to **Network > IVR**.

Step 2 Click **IVR Server > Transit** in the Manage IVR Server page.

Step 3 Click **Connect** to connect the PGW to the Movius VoiceMail system, for example: for connecting **PGW-ENT2** to **MoviusforCity2.**

Associating Movius VM Server with PGW

The PGW will be configured to route the calls to the selected Movius VoiceMail System. To associate the Movius VoiceMail System with the PGW do the following:

Step 1 Go to **Network >Voicemail Server.**

Step 2 Click **VoiceMail Server > Transit** in the Manage VoiceMail Servers page.

Step 3 Click **Connect** to connect the PGW to the Movius VoiceMail system, for example for connecting **PGW-ENT2** to **MoviusforCity2**.

Associating Unified CM Cluster with PGW for MWI Support

This is required in order to send the MWI signals to the Unified CM cluster. To associate the Movius VoiceMail System with the PGW do the following:

Step 1 Go to **Network > PBX Devices**.

Step 2 Click **Connectivity** corresponding to the Unified CM cluster name, for example: **e5c2.**

Step 3 Click **PBX > Transit.**

Step 4 Click **Connect** to associate the PGW with the Unified CM cluster, for example: for connecting **PGW-ENT5** to **e5c2.**

Note To enable Voicemail MWI support for a customer, the PBX system should be connected with Transit Switch by executing "ConnectIPPBXTransit" transaction so that bdigittree required routing MWI calls are configured on PGW. If the PBX (CUCM cluster) is already associated with PGW, then it has to be disconnected and connected again. While disconnecting the PBX->Transit association, if MML transaction on PGW fails stating “MWI related digittree configurations are missing in PGW”, then do the following,

- Change the PGW (Transit-switch) to manual mode and then disconnect PBX->Transit association.
- Before associating PGW with CUCM again, remove PGW manual config mode and then Connect PGW with CUCM.
  This should resolve the issue and relevant digittrees for MWI should have been provisioned properly on PGW.

Associating Unified CM Cluster with other Unified CM clustes

This is required if a custoimer VM Service is used on different locations in different clusters.

Procedure:

Step 1 Go to **Network > PBX Devices**.

Step 2 Click **Associated Devices button** corresponding to the CCM cluster that is used while creating the Hardware Group.

Step 3 Click **Add** in the Manage Device Set page.

Step 4 Enter the following details in the Add Device Set page.

- Set Name—<CCM-AssociatedSetVM>
- Description—<CCM-AssociatedSetVM>
- Transaction Type—<Add Voice Mail Service Pilot>

Step 5 Check the remaining **CCM Cluster** boxes.

Movius VoiceMail Customer Administration

This section describes required steps to define and configure a per-Customer VoiceMail service. In the Movius Voicemail system, a per-customer organization is created. The PGW is configured to handle per-customer Movius VoiceMail related calls.

Adding VoiceMail Service

For each customer that requires VoiceMail support, a VoiceMail service is created. To define a VoiceMail Service:

Step 1 Go to **Resources >VoiceMail Services**.

Step 2 Click **Add.**

Step 3 Enter the following details:

- Name—<uniquename>, for example **e3VMServiceCus1**
- Description—<VMServicedescription>, for example **VoiceMail Service City 3 Customer 1**
- Country—<country>, for example **United Kingdom**
- Site Code—<all9stolenghtofSLC>, for example **999**
- VoiceMail Server Hardware Group—<VMServerHwGrp>, for example **e5pgwipuhwrgrpclu2**
- Extension Length—<ExtLenght>, for example **3**
- VoiceMail PSTN Dial Prefix—<VMPSTNDialPrexif>, for example **9**

Step 4 Click **Next>>**

Step 5 Enter the following details:

- VoiceMail Server—<VMServer>, for example **MoviusforCity2**
- Click **Next >>**

Step 6 Click **Add**

Allocating Internal Number for VoiceMail Pilot Number

For each customer that requires Movius VoiceMail support, an internal number should be available so that it can be used for the VoiceMail Pilot number. To allocate an internal number:

Step 1 Go to **Resources >VoiceMail Services**.

Step 2 Select the configured VoiceMail service—**e3VMServiceCus1**.

Step 3 Click **Internal Number Mgt**.

Step 4 Verify that the desired Internal Number is available. If it is not available, click **Allow**.

Adding VoiceMail Pilot Number

For each customer that requires Movius VoiceMail support, an Organization is created in Movius to uniquely identify each customer. The Movius Organization is created when the VoiceMail Pilot Number is added. To add a VoiceMail pilot number:

Step 1 Go to **Resources >VoiceMail Services.**

Step 2 Select the configured VoiceMail service, for example **e3VMServiceCus1**

Step 3 Click **Pilot Number.**

Step 4 Click **Add**

Step 5 Enter the following details:

- Select Pilot Number—<PilotNumber>, for example **Extension Number 000**
- Domain Name—<DomainName>, for example **e5cus1.com**
- Time Zone—<TimeZone>, for example **Europe/London**

Step 6 Click **Add**

Note When the Movius VoiceMail Pilot Number is added, a Movius Organization is created in Movius. For handling MWI and Outgoing Calling the organization is associated to a Call Agent (PGW) based on the values specified through the model in the following fields:

```
<mwiCAID>101</mwiCAID>
<outgoingCAID>101</outgoingCAID>
```

where "101" represents the Call Agent ID.

Ensure that the Call Agent for MWI and Outgoing Calls are updated with proper Call Agents. If not updated properly, do the following for the newly created Organization under second CA whose ID is 102.

Step 1 Go to **Organization.**

Step 2 Select the newly created organization, for example **e3VMServiceCus1.**

Step 3 Click **Edit**

Step 4 In the Out Call, set the **Outgoing call Agent**, for example: **PGW-ENT3**

Step 5 In the Message Waiting Indication, set the **Default MWI Call Agent**, for example: **PGW-ENT3**

Step 6 Click **Update.**

Note Due to AXL API limitations, The USM cannot create the MWI On and MWI Off devices in Unified CM. Furthermore it provides no indication to the end user how to configure this, and MWI will not work without it. Currently, the only reliable method to determine these numbers is to log in to PGW as mgcusr, change directory to /opt/CiscoMGC/etc/cust_specific and to execute the following command to determine the MWI On and MWI Off numbers per cluster: grep "MWI O" *. For each CCM Cluster, it will be necessary to manually create an MWI ON & MWI OFF Device with these numbers. These numbers should be configured in the "AllowMWI" partition and the Output CSS should be set to "IncomingToCluster" as this will allow the devices to turn any IP Phone MWI light on or off. For example:

On the PGW:

```
pgw-ent8m% cd ../etc/cust*
pgw-ent8m% pwd
/opt/CiscoMGC/etc/cust_specific
pgw-ent8m% grep "MWI Os" *
10519aaaaaaa:;
```

001 Constant Digit string used within the "MWI On" number. The MWI On number on each cluster will be 109999666001 where the first 2 digits (i.e.10) is CPID of the CUCM cluster.

```
10519aaaaaaa:;
```

002 Constant Digit string used within the "MWI Off" number. The MWI Off number on each cluster will be 109999666002 where the first 2 digits (i.e.10) is CPID of the CUCM cluster.

Adding and Moving E.164 Number for VoiceMail Pilot Number

To enable users to access VoiceMail from PSTN, an E164 number has to be associated with the VoiceMail Pilot Number.

Procedure:

Step 1 Go to **Resources > E.164 Inventory**.

Step 2 Select a Country from the drop down list.

Step 3 Click **Next**.

Step 4 Select National Area Code—<areacode>, for example **1402**.

Step 5 Click **Next**.

Step 6 Click **Add Number**.

Step 7 Enter the following details in the E164 Telephone Number page:

- National Area Code— Leave the previously selected area code
- Local Number (in this Area)—<LocalNumber>, for example **610000**

Step 8 Click **Add**.

To make the E164 Number available to the Customer VoiceMail Service, do the following:

Step 1 Go to **Resources > E.164 Inventory**.

Step 2 Select a Country in the E164 Telephone Numbers page.

Step 3 Click **Next**

Step 4 Select National Area Code from the drop down list, for example **1630**.

Step 5 Click **Next**.

Step 6 Click **Move Number Range**.

Step 7 Enter the following details in the E164 Telephone Numbers page:

- Selected Location—Select the required customer VoiceMail service, for example **UKReseller1 : UK-Cust1 : e3VMSCust1 : e3VMSCust1**
- Start of Number Range—Select the previously created E164 number, for example **1402610000**
- End of Number Range—Select the same number, for example **1402610000**

Step 8 Click **Move.**

Associating E.164 Number to VoiceMail Pilot Number

The E.164 number created in the previous step can now be associated with the VoiceMail Pilot Number. To associate the E164 number with the VoiceMail pilot number to the following:

Step 1 Go to **Resources >VoiceMail Services**.

Step 2 Select the configured VoiceMail service, for example: **e5VMServiceCus1**

Step 3 Click **PSTN Number Mgt.**

Step 4 Click **Range Assoc.**

Step 5 Select the National Code, for example **1402**.

Step 6 Click **Next >>**

Step 7 Enter the following details:

For the Range Start and Range End select:

- Previously configured PSTN Number: <PSTNNumber>, for example **1402610000**
- Extension Number used for the VoiceMail Pilot Number <VMPilotEx>, for example **000**

Step 8 Click **Select**

Adding Default VoiceMail Class of Service

To add support for the Default Movius VoiceMail Class of service (CoS):

Step 1 Go to **Resources >VoiceMail Services**.

Step 2 Select the configured VoiceMail service, for example: **e5VMServiceCus1**

Step 3 Click **VoiceMail Profile Mgt**

Step 4 Check the **Standard VoiceMail** check box

Step 5 Click **Update**

Note Basic VoiceMail is not configured on Hosted UCS 7.1 (a) Model.

Movius VoiceMail Location Administration

This section describes required steps to define and configure a per-Location VoiceMail service. It also details how VoiceMail support is added to users.

Adding Location VoiceMail Service

For each location that requires VoiceMail support, the VoiceMail service created at the customer level is enabled. To add VoiceMail Service to a location:

Step 1 Go to **General Administration > Locations.**

Step 2 Select a VoiceMail support Location.

Step 3 Click **Advanced Mgt.**

Step 4 Click **VoiceMail Mgt.**

Step 5 Click **Add**

Step 6 Enter the following details:

- Name: <LocVMService>, for example **e3VMS1loc**1
- Select a VoiceMail Service: <CusVMService>, for example **e3VMSCus1**

Step 7 Click **Next**

Step 8 Select VoiceMail Pilot Number: <VMPilot>, for example **Extension Number 099**

Step 9 Click **Add and Enable.**

Note This action will cause disruption to end users

Adding VoiceMail Account to User

For each user that requires VoiceMail support, a VoiceMail account is created.

Caution Before a VoiceMail Account can be added to a user, the user should either be associated with a phone or have extension mobility.

To add a VoiceMail Account for a User do the following:

Step 1 Go to **Location Administration > Users**.

Step 2 Click **Add** corresponding to **Has VoiceMail** for the user you want to add a VoiceMail account (for example user1)

Step 3 Enter the following details:

- Password—<VMPassword>, for example **12345**
- Line Number—<LineNumber>, for example **004**
- Service Type—<ServiceType>, for example **StandardVoiceMail**

- Click **Add**

Note After provisioning VoiceMail for a phone user, the SIP lP links created on the PGW should be made In Service (IS), so that VoiceMail calls of phone user are routed to IP Unity Server. Execute the following MML command on the PGW. PGW-ENT2M mml> set-iplnk:moviussiplnk-*:IS

Sometimes, IP links does not come to "In Service" state. In such cases, restart the PGW MGC service.

For example,

```
PGW-ENT2M% su - root
Password:
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
# /etc/init.d/CiscoMGC stop
# /etc/init.d/CiscoMGC start
```

Provisioning Movius Auto Attendant

The Auto Attendant feature automatically answers all incoming calls to its pilot number and routes such calls to appropriate destinations based on the configured menu.

Hosted UCS Auto Attendant (AA) uses the same Voicemail Hardware [Movius (IP Unity) platform] to provide the Auto Attendant functionality. Licenses are required for Auto Attendant functionality.

USM performs the provisioning of the telephony part for Auto Attendant, for example, creating an Auto Attendant service and associating a pilot number for it. All Auto Attendant related configurations including setting Auto Attendant menus, uploading audio files, and defining actions based on DTMF input, are permormed through Movius web interface.

Be aware of the following important characteristics of Auto Attendant:

- Auto Attendant in Hosted UCS is based on Location and is dependent on Voicemail. For a location to have Auto Attendant, it must have Voicemail.
- Auto Attendant uses the same Voicemail SLC (Site Location Code)
- Multiple Pilot numbers can be assigned per Auto Attendant.
- Auto Attendant can have multiple menus.

Following Menu Features can be Configured in HUCS:

- Dial Configured Phone Number
- Play Announcement
- Announce and Disconnect
- Jump to Menu
- Jump to a different Auto Attendant
- Go Back to previous Menu
- Do Nothing
- Invalid Option

Auto Attendant Provisioning is carried out in the following phases:

Movius Auto Attendant configuration on USM

This section describes required steps to define and configure a per-Customer Auto Attendant service. Configure the VoiceMail services in a location before creating an Auto Attendant Service Pilot for a location. This section covers the following topics:

Adding Auto Attendant Service

For each customer requiring AA support, an AA service is created.

Procedure:

Step 1 Go to **Resources > Auto Attendant Services**.

Step 2 Click **Add**

Step 3 Enter the following details:

- Name—<uniquename>, for example **e3AAServiceCus1**
- Description—<AAservicedescription>, for example **AuttoAttendant Service City 3 Customer 1**
- Country—<country>, for example **United Kingdom**
- IVR Server Hardware Group—<VMServerHwGrp>, for example **pgw3-e3c4-hwgrp-ipunity**
- Click **Next >>**
- Select the IVR Server fom the drop-down list, for example: **MoviusforCity3**
- Click **Next >>**

Step 4 Click **Add.**

Allocating Internal Number for Auto Attendant Pilot Number

For each customer requiring Movius Auto Attendant support, an internal number should be available so that it can be used for the Auto Attendant Pilot number. The Auto Attendant pilots are extensions associated to a Voicemail Service. The Auto Attendant pilot that is created for a location is selected from the enabled extension from the Voicemail Service associated to the location.

Procedure:

Step 1 Go to **Resources > VoiceMail Services**.

Step 2 Select the VoiceMail service associated to the location, for example: **e3VMServiceCus1.**

Step 3 Click **Internal Number Mgt**.

Step 4 Verify that the desired Internal Number is available. If it is not available, click **Allow**.

Adding Auto Attendant Service Pilot Number

To create a pilot for an Auto Attendant Service on a customer, it is required to select a location. The location should have a VM Service associated to it, otherwise USM would not show any available extensions to select. The pilot number will be one of the extensions of that VM Service. If the extension that we want to use is not available then allow the internal number as explained in the topic Allocating Internal Number for Auto Attendant Pilot Number, page 6-20

Procedure:

Step 1 Select the configured Auto Attendant service, for example: **e3AAServiceCus1**

Step 2 Click **Pilot Numbers**

Step 3 Click **Add**

Step 4 Select a division and the location where we want to create that AA Service Pilot Number.

Note The location needs to have a VM Service allocated.

Step 5 Enter the following details:

- Select Pilot Number—<PilotNumber>, for example **Extension Number 098**
- Enter a Name—for example, **AACust1Div1Loc1**

Step 6 Click **Add.**

Figure 6-3 USM – Output of adding AA pilot for a location

Note The AA pilot FINT number **150100401099** is shown at the end in the above figure. Write down that number as it is required in the later steps.

Adding and Moving E164 Number for Auto Attendant Pilot Number

To enable users to access Auto Attendant from PSTN, an E164 number has to be associated with the Auto Attendant Service Pilot Number.

To add an E164 Number do the following:

Step 1 Go to **Resources > E.164 Inventory.**

Step 2 Select a Country from the drop-down list.

Step 3 Click **Next**

Step 4 Select National Area Code—<areacode>, for example **1630.**

Step 5 Click **Next**.

Step 6 Click **Add Number**.

Step 7 Enter the following details:

- National Area Code—Enter the previously selected area code
- Local Number (in this Area):<LocalNumber> for example, **610000**

Step 8 Click **Add**.

To make the E164 Number available for the AA, it needs to be made available to the Customer VoiceMail Service associated to the location.

Procedure

Step 1 Go to **Resources > E.164 Inventory.**

Step 2 Select a Country from the drop down list.

Step 3 Click **Next.**

Step 4 Select National Area Code—<areacode> for example, **1630**.

Step 5 Click **Next**.

Step 6 Click **Move Number Range**.

Step 7 Enter the following details:

- Selected Location—Select the required Customer VoiceMail Service, for example **UKReseller1 : UK-Cust1 : e3VMSCust1 : e3VMSCust1**
- Start of Number Range—Select the Previously created E164 number, for example **1630610000**
- End of Number Range—Select the same Select the same number, for example **1630610000**

Step 8 Click **Move.**

Associating E.164 Number to Auto Attendant Pilot Number

The E.164 number created in the previous step can now be associated with the Auto Attendant Pilot Number.

Procedure:

Step 1 Go to **Resources >VoiceMail Services.**

> **Note** Ensure that you are associating the E.164 number to the VoiceMail Pilot Number for the correct Customer.

Step 2 Select the configured VoiceMail service; for example, **e5VMServiceCus1**

Step 3 Click **PSTN Number Mgt.**

Step 4 Click **Associate Range.**

Step 5 Select the National Code, for example **1402**

Step 6 Click **Next >>**

Step 7 Enter the following details:

- Range Start—Select Previously configured PSTN Number: <PSTNNumber>, for example **1630610000**
- Range End—select the same PSTN Number if you want to associate a single PSTN number to an extension otherwise select the PSTN range end. In this case, **1630610000**
- Extension Number used for the AutoAttendant Pilot Number <AAPilotEx>, for example **000** for both Range start and Range end
- Click **Submit**

Repeat this step for all Customers using the Movius VoiceMail system on all Hosted UCS platforms (Providers).

Auto Attendant configuration on Movius server

This section explains how to configure the Auto Attendant on the Movius server. The following topics are explained in this section.

- Creation of Auto Attendant on Movius organization., page 6-24
- Adding AA Announcement File, page 6-26
- Configuring a Menu for the AA, page 6-27
- Adding FSM Keys., page 6-28

Creation of Auto Attendant on Movius organization.

We should know the organization where we have to create the AA. On non-shared building locations, the organization name is same as the Voicemail Service. We have to know the name of this Voicemail service in order to find the organization on the Movius Server. To know the Location where a pilot is created do the following:

Step 1 Go to **Resources > Auto Attendant Services**

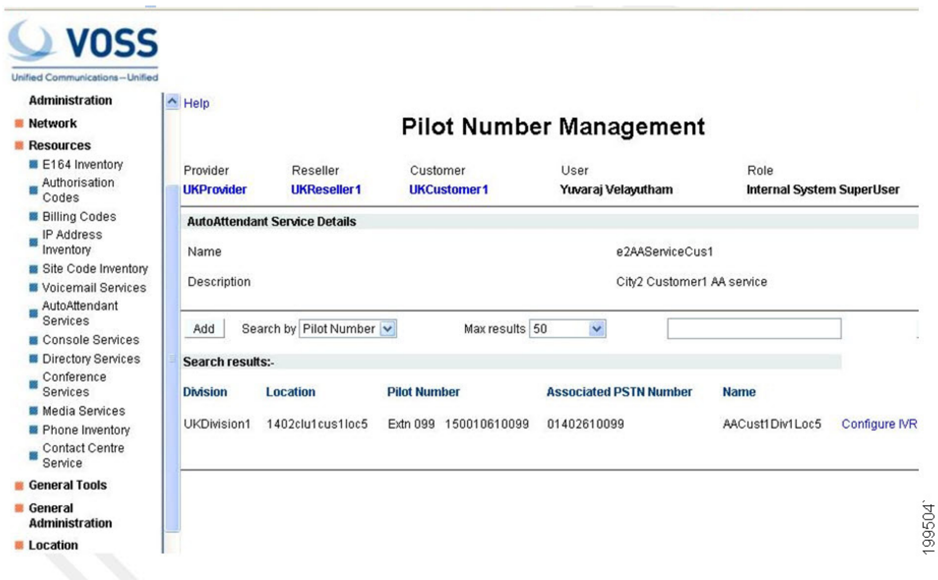
Step 2 Select the customer of the AA Service.

Step 3 Select the AA Service where we created a pilot , for example **e3AAS2Cust1**

Step 4 Click **Pilot Numbers**

All pilots created for an AA Service with the location where they were created and the FINT of the pilot Number are shown in the figure below:

Figure 6-4 USM Server – List of pilots for an AA Service. FINT number of Pilot highlighted.



To know the name of the organization do the following:

Step 1 Go to **General Administration > Locations**.

Step 2 Select location where the AA Service Pilot is created

Step 3 Click **Advanced Mgt.**

Step 4 Click **VoiceMail Mgt.**

On right column we can see the VoiceMail Service Name associated to that location. This is the name of the organization created on Movius.

Once we gathered all these information, we can log into Movius Mereon UM Configuration page. The system configuration page can be accessed via:

http://<IP_Unity_GUI_IP_Address>/sysconfig/webconfig/login-javascript.jsp

Note For the HUCS Solution test Movius VoiceMail System 4.2, the following IP address, Username, and password can be used:

- NAT IP—**10.78.97.70** (Internal IP: 10.100.91.72)
- Username—**system**
- Password—**ipunity**

To create an Auto Attendant on the organization do the following:

Step 1 Go to **Organizations** on the left side menu and search for the organization with the same name as the VM Service (i.e e3VMS2).

Step 2 Click **Login.**

Step 3 When prompted <Organization>, click **OK.**

Step 4 Select **Auto Attendant** on left side menu.

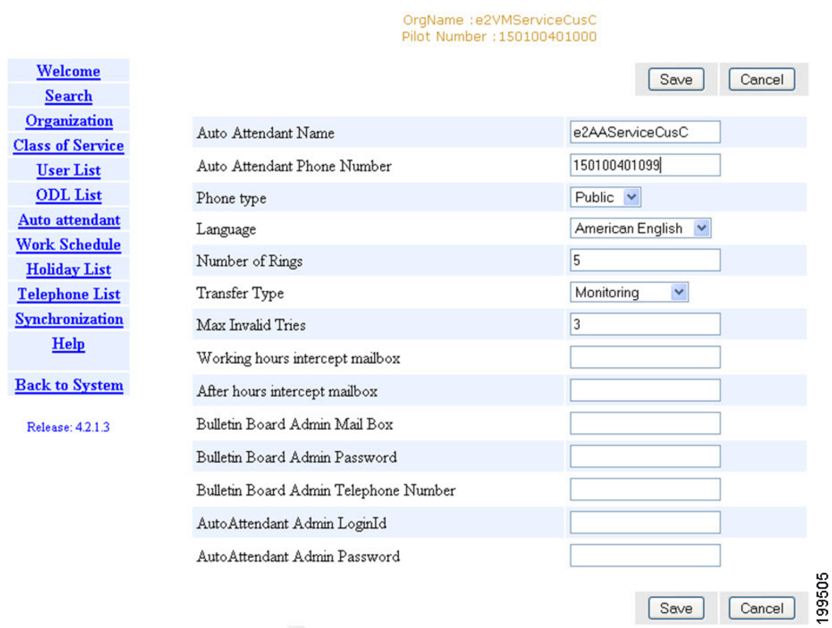
Step 5 Click **Add**.

Step 6 Enter the following:

- Auto Attendant name—for example, **e3AAServiceCust1**
- Auto Attendant Phone Number—for example, **150100401099** (Enter the FINT number of the pilot)
- Phone Type—**Public**
- Transfer Type—Monitoring

Step 7 Click **Save.**

Figure 6-5 Mereon UM Configuration – Adding an Auto Attendant in an organization.



Adding AA Announcement File

Note Auto Attendant announcement can be an administrator recorded audio file based on requirements or the administrator can use the default announcement file supplied by Movius.

The following steps show how to add an announcement file to an Auto Attendant service.

Step 1 Click **Auto attendant** on the left side menu.

Step 2 Click **Announcement Management**.

Step 3 Click **Add,** to add a single announcement file.

Step 4 Enter the name of the announcement file ending with ".wav" and click **OK**.

Step 5 Click **Upload**.

Step 6 Browse the file from the local machine and click **Upload Announcement.**

Configuring a Menu for the AA

Once created the Auto Attendant, we can configure the menu for this Auto Attendant. The menu should be configured depending on the requirements of the client.

For the announcement prompted when the AA is dialled, click on Announcement Management to import the different wave files.

If you want the announcement to be played when the user dials AA pilot number, configure the menu:

Procedure:

Step 1 Click **Menu Configuration** on the respective Auto attendant service

Step 2 Click **Menu** which is already added. If not, add a new menu.

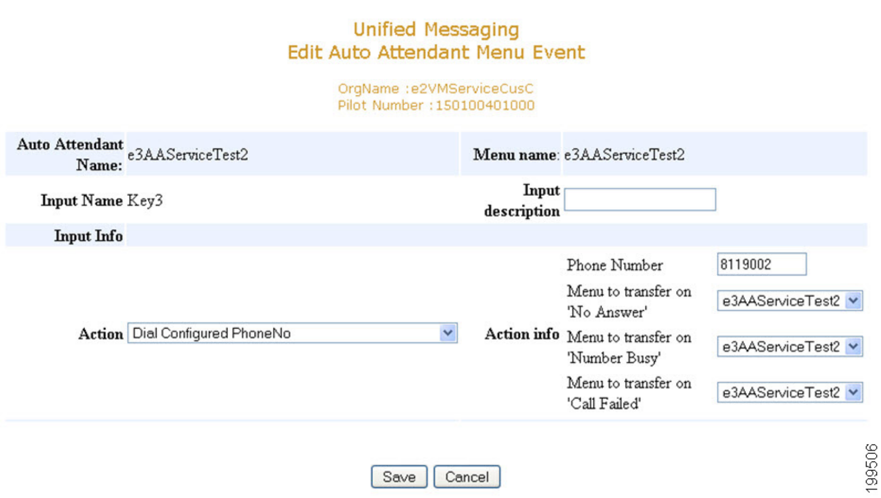
Step 3 Click **Edit Configuration Parameters** in the Menu Configuration page.

Step 4 Click **Configure Initial Action**

Step 5 On the pop-up GUI, select the action **Play Announcement** and Add announcement file name.

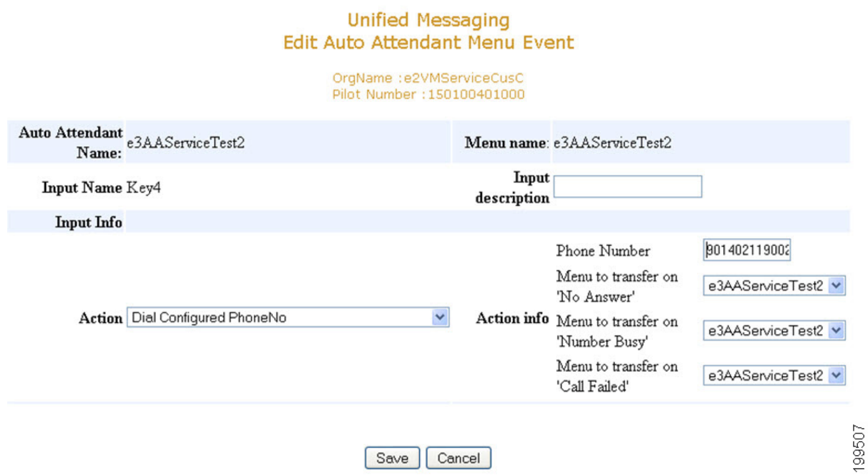
The figure 6-6 below illustrates configuring AA to dial 8119002 by pressing 3, for example, when the intersite prefix is 8 and the extension number is 002 in the location 119.

Figure 6-6 Movius UM Configuration - Configuring AA to dial 8119002 when presssing 3



The figure 6-7, below illustrates configuring AA to dial 901402119001 by pressing 4, for example, when the PSTN breakout code is 9 and the PSTN Number is 01402119002.

Figure 6-7 Movius UM Configuration - AA to dial 901402119002 when pressing 4



Adding FSM Keys.

Log into Movius OAM Configuration page. The system configuration page can be accessed via: http://<IP_Unity_GUI_IP_Address>/oam

Note For the HUCS Solution Test Movius VoiceMail System 4.2, the following IP address, Username, and password can be used:

- NAT IP—**10.78.97.70** (Internal IP: 10.100.91.72)
- Username— **ipunity**
- Password—**ipunity**

To create an Auto Attendant on the organization do the following:

Step 1 Go to **Configuration > Framework Configuration > Framework Application Parameters > ipunity.apps.vm.UMApp > ipunity.apps.vm.AutoAttendantCall > FSM Keys**

Step 2 Click **Add**

Step 3 Enter the following:

- App Key—Enter FINT number of the AA Pilot number
- Node—**Virtual IP**

Step 4 Click **Update.**

Provisioning Movius Auto Attendant with SBC

This section describes the provisioning steps required to configure SBC, PGW and Movius. The following topics are covered in this section:

- SBC Configuration in ASR 1002, page 6-29
- Movius AA Configuration, page 6-32
- PGW Configuration, page 6-32

SBC Configuration in ASR 1002

This topic describes the steps required to configure ASR 1002 as Session Boarder Controller.

- Create a SBC Interface, page 6-29
- Create SIP Profiles and Headers, page 6-29
- Create SIP adjacency for PGW and Movius, page 6-30
- Create Codec List, Cac policy and Call policy, page 6-31
- Create Media Address for SBC, page 6-32

Create a SBC Interface

Access ASR 1002 through telnet session and use the following command to create SBC interface which will be used for signalling and media by SBC.

```
interface SBC0
    ip address 100.1.1.20 255.255.255.0 secondary //IP Address to be used for media
    ip address 100.1.1.10 255.255.255.0
!
interface GigabitEthernet0/0/0
    description to city2sbc
    ip address 10.190.1.50 255.255.255.0 secondary //IP Address to be used for signalling
    ip address 10.190.1.46 255.255.255.0 //Primary Interface address
    negotiation auto
    no mop enabled
!
```

Create SIP Profiles and Headers

Use the following commands to create SIP Profiles and Headers.

```
sbc city2sbc //city2sbc is the SBC name
 sbe
   sip header-profile headerprofile1
    description pass session-expiry header
    header Allow entry 1
     action as-profile
    header Reason entry 1
     action as-profile
    header SERVER entry 1
     action as-profile
    header DIVERSION entry 1
     action as-profile
    header Allow-Events entry 1
     action as-profile
```

```
    header session-expiry entry 1
     action as-profile
    header Remote-Party-ID entry 1
     action as-profile
    header Session-Expires entry 1
     action as-profile
    header RESOURCE-PRIORITY entry 1
     action as-profile
    header P-Asserted-Identity entry 1
     action as-profile
   sip method-profile method1
    description pass default methods
    pass-body
    method INFO
     action as-profile
    method PRACK
     action pass
    method REFER
     action as-profile
    method NOTIFY
     action as-profile
    method UPDATE
     action as-profile
    method SUBSCRIBE
     action as-profile
   sip option-profile option1
    description pass default options plus timer
    option TIMER
    option REPLACES
```

Create SIP adjacency for PGW and Movius

Two SIP adjacencies are needed to interact with PGW and Movius. Following commands are used to create the adjacencies. The SIP headers and profiles created in the previous section are attached in both the adjacencies.

```
sbc city2sbc
 sbe
    adjacency sip pgw //pgw - adjacency name to interact with PGW
        force-signaling-peer
        nat force-on
        preferred-transport udp
        signaling-address ipv4 10.190.1.50//Ip address created in sec 2.1 for signalling
        statistics method summary
        signaling-port 5060
        remote-address ipv4 10.120.2.0 255.255.255.0 //Ip address for PGW
        signaling-peer 10.120.2.13 //Ip address of PGW
        account pgw
        sipi passthrough
        media-late-to-early-iw outgoing
        attach
    adjacency sip movius //movius - adjacency name to interact with Movius
        force-signaling-peer
        nat force-on
        header-profile inbound headerprofile1
        header-profile outbound headerprofile1
        method-profile inbound method1
        method-profile outbound method1
        option-profile ua inbound option1
        option-profile ua outbound option1
        preferred-transport udp
```

```
        signaling-address ipv4 10.190.1.50 //Ip address created in sec 2.1 for signalling
        statistics method summary
        signaling-port 5060
        remote-address ipv4 10.100.91.0 255.255.255.0 //Ip address for Movius
        signaling-peer 10.100.91.72 //Ip address of Movius
        account movius
        sipi passthrough
        media-late-to-early-iw incoming
        media-late-to-early-iw outgoing
        attach
```

Create Codec List, Cac policy and Call policy

Following commands are used to create the codec list, active call policy and the cac policy.

```
cac-policy-set 1
    first-cac-table table
    first-cac-scope call
    cac-table table
    table-type limit account
    entry 1
        match-value movius
        max-bandwidth-per-scope 64009 Gbps
        max-updates-per-call 429496729
        max-channels-per-scope 429496729
        caller-codec-list allowcodec
        callee-codec-list allowcodec
        callee-hold-setting hold-c0
        caller-hold-setting hold-c0
        action cac-complete
    entry 2
        match-value pgw
        max-bandwidth-per-scope 64009 Gbps
        max-updates-per-call 429496729
        max-channels-per-scope 429496729
        caller-codec-list allowcodec
        callee-codec-list allowcodec
        callee-hold-setting hold-c0
        caller-hold-setting hold-c0
        action cac-complete
    complete
    active-cac-policy-set 1
    call-policy-set 1
    first-call-routing-table start-table
    rtg-src-adjacency-table start-table
    entry 1
        action complete
        dst-adjacency pgw
        match-adjacency movius
    entry 2
        action complete
        dst-adjacency movius
        match-adjacency pgw
        complete
    active-call-policy-set 1
    sip timer
    udp-response-linger-period 5000
!
!
    codec list allowcodec
        codec telephone-event
        codec PCMU
!
```

Create Media Address for SBC

Following commands are used to create the media address.

```
sbc city2sbc
    media-address ipv4 100.1.1.20
    activate
```

Movius AA Configuration

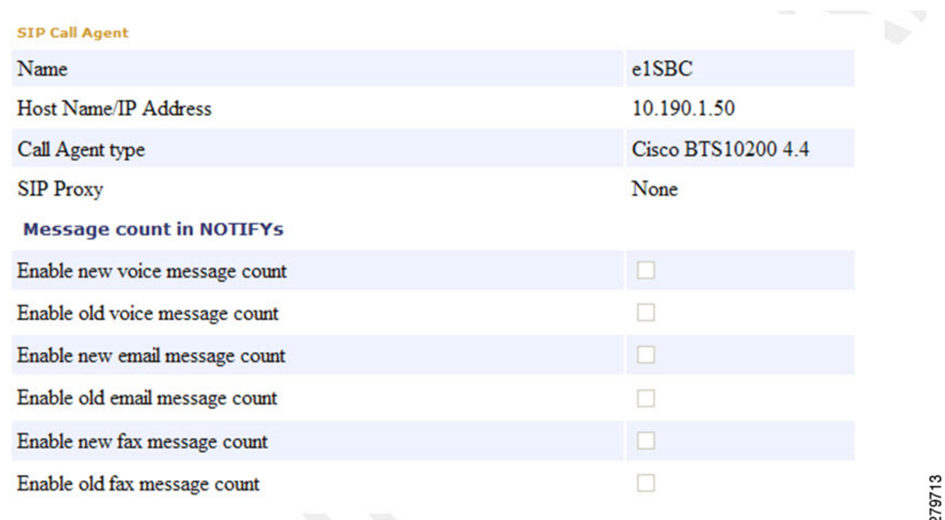
This topic describes the required steps to edit the configuration in Movius Auto Attendant to work with SBC. Before editing any configuration, configure the movius auto attendant and voice mail using the document "HUCS_7_1_A-Movius_VM_and_AA_Provisioning_Guide.doc". Make sure the auto attendant and voice mail calls are working successfully with Cisco PGW as call agent in movius (Without SBC).

If the AA and Voice mail calls are working successfully, use following steps to edit the configuration to work with SBC.

Step 1 Click on "Call Agent" on the left hand side menu and then click "SIP Call Agent".

Step 2 Add one SIP Call Agent for SBC as shown below and click on "Save" button.

Figure 6-8 Add SIP call Agent for SBC



Step 3 Click on "Organization" and select the previously created Organization.

Step 4 Click on "Edit" to modify the "Outgoing Call Agent" to "e1SBC". To save the changes, click on "Update".

PGW Configuration

This topic describes the required steps to modify the configuration in Cisco PGW to integrate Movius Auto Attendant and SBC. Before making any changes, make sure the Auto Attendant and voice mail calls are working fine without SBC.

- Log on to Cisco PGW as mgcusr and type “mml” and press “Enter”.
- Check the configured SIP profiles using the following command and use the same sip profile name in the next step.
  mml> prov-rtrv:profile:"all"
- Use the following commands to disable 183 Support and enable 100rel support in the sip profiles.

```
mml> prov-sta::srcver="active",dstver="AASbc_config1"
mml>prov-ed:profile:name="moviusippf3001",type="SIPPROFILE",support183="0",supportreliable
100="SUPPORTED"
mml>prov-ed:profile:name="moviusippf3002",type="SIPPROFILE",support183="0"
mml> prov-cpy
mml> quit
```

CHAPTER 7

Provisioning the Local PSTN Breakout Support

This document details how PSTN calls can be routed via Local Gateways in the Hosted UCS reference architecture for the Hosted UCS 7.1(a) Release. It also provides steps required to provision the Local PSTN Breakout feature via the VOSS USM application.

In Hosted UCS 7.1(a) Release, the administrator can provision Local Gateways for a customer location. Calls to/from PSTN can be routed via PRI or BRI interfaces. The format of the Calling and Called party number and Nature of Address (NOA) can also be configured in various ways. Additionally, calls to/from PSTN from one location can be routed via a single trunk, or optionally, the administrator can provision two trunks to separate Local and National/International calls.

This chapter is divided into the following sections:

- Description of the Local PSTN Breakout Support, page 7-1
- Provisioning Local PSTN Breakout Support, page 7-7

Description of the Local PSTN Breakout Support

This section describes the key characteristics of the Local PSTN Breakout Support feature:

- Handling PSTN Calls via Central Gateway, page 7-1
- Handling PSTN Calls via Local Gateway, page 7-4
- Support for Multiple Trunk Types for Local PSTN Breakout, page 7-7

Handling PSTN Calls via Central Gateway

In Cisco Hosted Unified Communications Services 7.1(a), you can provision a location, so that calls to the PSTN are sent via a Central Gateway.

Table 7-1 lists the generic formats of the cgpn (A), cgpn nature of address (ANOA), cdpn (B), and the cdpn NOA (BNOA) on the Central Gateway trunk when a location is provisioned to route PSTN calls via a central gateway.

Table 7-1 Outgoing calls to PSTN via Central Gateway

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local Call	NDC1-SN2	National	NDC-SN	National

Table 7-1 Outgoing calls to PSTN via Central Gateway

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
National Call	NDC-SN	National	NDC-SN	National
International Calls	NDC-SN	National	CC3-NDC-SN	International

Table 7-2 lists the generic expected formats of the cgpn (A), cgpn nature of address (ANOA), cdpn (B), and the cdpn NOA (BNOA) on the Central Gateway trunk for incoming calls from PSTN.

Table 7-2 Incoming calls from PSTN via Central Gateway

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local Call	NDC-SN	National	NDC-SN	National
National Call	NDC-SN	National	NDC-SN	National
International Calls	CC-NDC-SN	International	NDC-SN	National

In the US for example, the North American Numbering Plan (NANP) is used. The NANP number is a 10-digit number that consists of the following three parts:

- 3-digit Numbering Plan Area (NPA) code
- 3-digit Central Office (CO) code
- 4-digit line (or station) number

The format of the NANP number is NXX-NXX-XXXX4 (the use of the NPA code is optional in some areas that permit 7-digit local dialing). To avoid confusion between the NPA and CO codes, the NANP numbers in this document will be presented with NPA-NXX-XXXX.

Table 7-3 lists the generic formats of the cgpn (A), cgpn nature of address (ANOA), cdpn (B), and the cdpn NOA (BNOA) on the Central Gateway trunk in the US.

Table 7-3 Outgoing calls from PSTN via Central Gateway in the United States

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local call from 7-digit location	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
Local call from 10-digit location	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
Long distance call	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
International Calls	NPA-NXX-XXXX	National	CC-E164	International

National Destination Code (NDC/NPA) - A nationally optional code field, within the international E.164-numbering plan. The NDC has a network and/or trunk code selection function. The NDC can be a decimal digit or a combination of decimal digits (not including any prefix) identifying a numbering area within a country (or group of countries included in one integrated numbering plan or a specific geographic area) and/or network/services.

Subscriber Number (SN) - The portion of the international E.164-number that identifies a subscriber in a network or numbering area.

Country Code (CC)/National Access Code (NAC) - The combination of one, two or three digits identifying a specific country in an integrated numbering plan, or a specific geographic area.

Note N can be any digits from 2 to 9, and X can be any digits from 0 to 9

Table 7-4 lists the generic expected formats of the cgpn (A), cgpn nature of address (ANOA), cdpn (B), and the cdpn NOA (BNOA) on the Central Gateway trunk for incoming calls from PSTN for the US.

Table 7-4 Incoming calls from PSTN via Central Gateway in the United States

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local call from 7-digit location	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
Local call from 10-digit location	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
Long distance call	NPA-NXX-XXXX	National	NPA-NXX-XXXX	National
International Calls	CC-E164	International	NPA-NXX-XXXX	National

Note Be aware that these are generic numbering formats, and if different formats are required the SI can customize the Ingress and Egress PGW dial plans (P#PADDEDCC# and F#PADDEDCC# dial plans).

Table 7-5 lists the generic expected formats of the the cdpn (B) to NXX-XXXX (for local calls from locations provisioned for 7-digit local dialing support), or to NPA-NXX-XXXX (for local calls from locations provisioned for 10-digit local dialing support), and BNOA to subscriber, on the Central Gateway trunk for outgoing calls to PSTN for the US.

Table 7-5 Customized outgoing local calls to PSTN via Central Gateway in the United States

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local call from 7-digit location	NPA-NXX-XXXX	National	NXX-XXXX	Subscriber
Local call from 10-digit location	NPA-NXX-XXXX	National	NPA-NXX-XXXX	Subscriber

Table 7-6 lists the generic expected formats of the the cdpn (B) to NXX-XXXX (for local calls from locations provisioned for 7-digit local dialing support), or to NPA-NXX-XXXX (for local calls from locations provisioned for 10-digit local dialing support), and BNOA to subscriber, on the Central Gateway trunk for incoming calls to PSTN for the US.

Table 7-6 Customized incoming local calls to PSTN via Central Gateway in the United States

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
Local call from 7-digit location	NPA-NXX-XXX X	National	NXX-XXXX	Subscriber
Local call from 10-digit location	NPA-NXX-XXX X	National	NPA-NXX-XX XX	Subscriber

Handling PSTN Calls via Local Gateway

In Cisco Hosted Unified Communications Services 7.1(a), you can provision a location to route PSTN calls via local gateway trunk(s). One, or optionally two, Local Gateway trunks can be provisioned in a number of ways that will enable sending and receiving of the cdpn (B) and BNOA in various formats. This section contains the following topics:

- Call Admission Control, page 7-4
- Calling and Called Party Number Presentation, page 7-4
- Call Routing, page 7-6

Call Admission Control

In HUCS7.1 (a) release, all calls from IP Phones to PSTN and from PSTN to IP Phones are routed directly via Unified CM therefore enabling the correct Call Admission Control (CAC) functionality. The LGW dedicated to a location is configured in Unified Communication Manager as an H.323 gateway and is configured in the same device pool as the IP Phones. Therefore, the Unified Communication Manager location bandwidth is not consumed for calls from IP Phones to LGW and from LGW to IP Phones.

Calling and Called Party Number Presentation

For all call scenarios that traverse the LGW, appropriate configuration can be applied to Unified Communication Manager and LGW to ensure that the Calling Party Number (CgPN) and Called Party Number (CdPN) are presented to the PSTN, the IP Phone or Movius in the required format.

The presentation of the CgPN and CdPN can be configured in a number of ways to satisfy Service Provider requirements for various call scenarios.

For outgoing Emergency calls:

- If the location is configured to use the Cisco Emergency Responder feature, the CgPN number is modified to the Emergency Location Identification Number (ELIN).
- If the location is configured to use the DDI for Emergency feature, the CgPN will be replaced with an E.164 number of the line which originated the call (if the line is associated with an E.164 number) or with the Location Emergency Published Number (if the line is not associated with an E.164 number).
- If the location is not configured to use the Cisco Emergency Responder or DDI for Emergency feature, the CgPN will always be replaced with the Location Emergency Published Number.

For outgoing Non-Emergency PSTN calls, the CgPN will be replaced with an E.164 number of the line which originated the call (if the line is associated with an E.164 number) or with the Location PSTN Published Number (if the line is not associated with an E.164 number).

For outgoing PSTN calls, each trunk can be configured to set the desired NOA, that is the CgPN NOA and CdPN NOA can be set to relevant National/International/Subscriber/Unknown format or Unknown for all call types.

In addition to this, the administrator can configure the trunk to choose:

- No Local Dialing
- 10-digit dialing (for US only) or
- Local Dialing without Area Code (for countries that can support this - 7-digit dialing).

If No Local Dialing is configured then local calls would be sent to and expected to be received from the PSTN trunk in the same way as national calls.

If 10-digit dialing is configured then local calls would be sent to and expected to be received from the PSTN trunk with the NDC.

If Local Dialing without Area Code is configured then local calls would be sent to and expected to be received from the PSTN without the NDC.

For example, in the US:

- National calls can be sent to the PSTN with:
  - 212-5551234 and NOA set to National or
  - 1-212-5551234 and NOA set to Unknown
- International calls can be sent to the PSTN with:
  - 44-1632-123456 and NOA set to International or
  - 011-44-1632-123456 and NOA set to Unknown
- Local calls can be sent to the PSTN with:
  - 5551234 and NOA set to Subscriber (for 7-digit dialing with NDC configured not to be sent),
  - 212-5551234 and NOA set to Subscriber (for 10-digit dialing or 7-digit dialing with NDC configured to be sent) or
  - 1-212-5551234 and NOA set to Unknown

For incoming calls to IP Phones, the CdPN will be replaced with an Internal number of the line (if the line is associated with an E.164 number) so that the call can be routed to the correct IP Phone. Also, the CgPN will be prefixed with the correct PSTN Access Prefix and relevant Access Code so that the user can redial the number if required.

For incoming PSAP call-back calls, if the location is configured to use Cisco ER feature then the CdPN (ELIN) will be replaced with an Internal number (every ELIN is associated to an internal number), so that the call can be routed to the correct Cisco ER.

For incoming calls to Movius (for Voicemail retrieval), the CdPN (E.164 number of the Voicemail pilot allocated to the LGW) will be replaced with an Internal number (every E.164 Voicemail pilot number is associated to an internal number), so that the call can be routed to Movius via Unified CM and PGW.

In cases where a user has dialed the E164 number of a phone within the same location then the CdPN number will be transformed to the relevant internal number so that the call can be routed to the correct IP Phone. Also, the CgPN number will be modified to 8+SLC+EXT, so that the user can identify this as an internal call and be able to redial the number if required. In addition to this, the CLI restriction will be removed if it is applied to the initial outgoing call.

When a call is forwarded to the Local PSTN Gateway:

- If the location is configured to use the DDI for Redirect feature, the CgPN will be replaced with an E.164 number of the line which redirected the call (if the line is associated with an E.164 number) or with the Location PSTN Published Number (if the line is not associated with an E.164 number)
- If the location is not configured to use the DDI for Emergency feature, the CgPN will always be replaced with the Location PSTN Published Number of the line which redirected the call.

In US, there is a distinction between national dialing, local dialing with the NDC (10-digit dialing) and local dialing without the NDC (7-digit dialing). Therefore, Local Gateway trunks can be configured for:

- No Local Dialing—This will result in local calls presented to the PSTN trunk in the same way as national calls.
- 10-digit dialing—This will result in local calls presented to the PSTN with the NDC.
- Local Dialing without Area Code—This will result in local calls presented to the PSTN without the NDC.

Additionally, for all countries, the Local Gateway trunks can be configured to set the Called Party Number (cdpn) B Nature of Address (BNOA) and Calling Party Number (cgpn) A Nature of Address (ANOA) as:

- NOA - Yes— In this case the cgpn and cdpn is set in a relevant format together with appropriate NOA based on the calling number and called destination.
- NOA - No— In this case the NOA is set to Unknown. Both cgpn and cdpn are prefixed with appropriate leading digits to distinguish calling number and called destinations.

For detailed information on all supported call scenarios and numbering presentation, please refer Appendix E, "Local Gateway Supported Call Scenarios".

Call Routing

Administrators can configure the PSTN call type for each country, from the following predefined call types:

- National
- International
- Emergency
- Service
- Local
- Mobile
- Toll-free
- Premium
- Low-cost

Fo each location, the administrator can configure to route these call types via Local or Central PSTN breakout. In addition to this, the administrator can select one more call types to be routable for each Local PSTN Gateway trunk.

The locations can be configured to support:

- 7-digit, 10-digit and 11-digit local dialing or
- 10-digit and 11-digit local dialing.

Support for Multiple Trunk Types for Local PSTN Breakout

In Cisco Hosted Unified Communications Services 7.1(a), it is possible to configure the LGW with multiple trunks. Each trunk can route one or more administrator defined PSTN call types. In addition to this the supported trunk interfaces are PRI and BRI.

For details on configuring a local gateway to support PRI or BRI trunk types, refer the section Define Local Gateway Interfaces.

Provisioning Local PSTN Breakout Support

This section describes required steps to provision Local PSTN Breakout support using Local Gateways:

Static Configuration

This section details the initial static (manual) configuration required for Local PSTN breakout support for the Local Gateway Static Configuration.

Local Gateway Static Configuration

It is assumed the Cisco IOS device at the customer location will require some level of manual configuration prior to configuring via VOSS-USM. This is typically the IP and access configuration, known as the base configuration, for example it should be configured with a physical or logical loop back interface which will be used as source of the H.323 traffic to Unified Communication Manager. IP configuration must ensure that if loop back interface is configured then the loop back interface can be reached through any of the two physical interfaces. This is possible by enabling routing protocol and configuring it consistently with the core network routing policies.

Furthermore, in Hosted UCS 7.1(a), a number of TCL applications developed by Cisco are used to take over the role of the Default application (the Default application is used to control voice dial-peers in IOS, which is part of IOS' built-in call control that basically binds two call legs whose characteristics are defined by the configured voice dial-peers). These applications are then configured on each voice dial-peer and each verifies on each voice call whether calling and/or called number needs to be translated in the same way as the voice translation-rules did in previous Hosted UCS release. Therefore it is necessary to download these TCL applications into the Voice gateway flash.

Use the following procedure to download the TCl applications:

Procedure:

Step 1 Download the tar file to a (t)ftp server, which contains the Hosted UCS 7.1.1 lite TCL applications.

Note If you are using FTP then you will have to use IOS commands to create telnet username and password, for example

- ip ftp username <xxx>
- ip ftp password <yyy>

Step 2 On the Local Gateway, execute the following command in priviledged EXEC mode:

<hostname>**#archive tar /xtract (t)ftp://<host>/<file.tar> flash:**; for example:

```
e41gw1#archive tar /xtract tftp://10.100.100.2/LocalGatewayTCL/hucstcl_v1.0-5.tar flash
```

<hostname>#call application voice load hucsntpstn

<hostname>#conf terminal

<hostname>#application

<hostname>#service hucsntpstn flash:hucsntpstn.tc

<hostname>#call application voice load hucsntvoip

<hostname>#conf terminal

<hostname>#application

<hostname>#service hucsntvoip flash:hucsntvoip.tcl

Repeat this procedure for all Local Gateways.

Loading the IOS Model

Note Ignore this step if the IOS Device model is already loaded on to USM. If the IOS Device model used with USM version 7.1.3 is country specific then appropriate country IOS Device model should be loaded on to USM.

This section describes required steps to load the Hosted UCS 7.1(a) IOS model. This model defines how USM should configure the Local Gateways.

The IOS command **voice service voip** in the IOS Device 12.x - Model H323 is not provisioned on local gateway if the gateway is provisioned via USM using telnet.

To solve this issue, the relevant IOS commands should be commented (if not already commented out) on the IOS model IOS Device 12.x - Model H323 worksheet before loading the model.

Procedure:

Step 1 Comment out the following lines (3 - 10) in the IOS Device 12.x - Model H323 worksheet

Step 2 Change the first column of the line 11 from A to I as shown below

```
# HUCS AddH323 voice service voip #EOL#
# HUCS AddH323 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none #EOL#
# HUCS AddH323 modem passthrough nse codec g711ulaw #EOL#
# HUCS AddH323 allow-connections h323 to h323 #EOL#
# HUCS AddH323 h323 #EOL#
# HUCS AddH323 emptycapability #EOL#
# HUCS AddH323 h245 passthru tcsnonstd-passthru #EOL#
# HUCS AddH323 ! #EOL#
I HUCS AddH323 voice class codec 1 #EOL#
```

Step 3 Save the model.

To prepare USM by loading the IOS Device model, use the following procedure:

Procedure:

Step 1 Choose **Dialplan Tools > Configuration Models**.

Step 2 Browse for the model loader being used, and click **Submit**.

Note Check for any errors or warnings once the loading completes.

Define Call Routing Types in USM

Call routing for call types routed via local gateway are defined as service types in USM. Call Routing Types can be defined in VOSS as service types, having a service category of gatewaycallrouting.

To add a new service type or to look at the existing service types, go to **Setup Tools > Service Types.**

A set of call routing types is available by default in USM. The table below lists the call routing types available, by default, in USM.

Table 7-7 Default Call Routing Services Types supported by USM

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

Add Call Routing Types to Country

Call routing types available in USM should be made available for the countries supported by provider for local gateway call routing. To enable call routing types for a country, do the following:

Step 1 Go to **Dial Plan Tools > Countries.**

Step 2 Select the country to which you want to add call routing types. For example, **United Kingdom.**

Step 3 Under **Supported Gateway Call Routing Type**, select all the call routing types which are required for that country, for example check the **check box** for the call routing types in Table 7.

Step 4 Click **Modify.**

Add Service Type for Incoming calls

Note If the Base-data sheet loaded into USM does not have the Service type IncomingToLGW, then you need to add that service type to map with a Cisco Unified Communication Manager (CUCM) CSS for incoming calls to LGW.

Load the BaseData-Append worksheet on to USM, if it is provided along with the model or follow the steps below to add IncomingToLGW service type:

Step 1 Go to **Setup Tools > Service Types.**

Step 2 Click **Add.**

Step 3 Under **Details**, enter the following:

- Service Name—<ServiceTypeName>, it should be **IncomingToLGW**
- Description—<ServiceDescription>, for example, **Incoming Call to Local PSTN Gateway**
- Tag—<ServiceTag>, for example, **IncomingToLGW**
- Service Category—<ServiceCategory>, select **outbound**

Step 4 Click **Add.**

Adding and Configuring Local Gateways

The administrator needs to follow the following steps to define and configure Local Gateways, at Provider level.

- Add IOS Device, page 7-11
- Define Local Gateways, page 7-11
- Configure Gateway Hardware, page 7-12
- Define Local Gateway Interfaces, page 7-13

Add IOS Device

To add an IOS Device Type:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click **Add**.

Step 3 Click **Add** corresponding to **IPPBX Connected H.323 Local Gateway.**

Step 4 Under **Device Details**, enter the following :

- Host Name—<Host name of the IOS Device>, for example **e2lgw1**
- Description—<IOSDeviceTypeDesc>, for example **City2 location2 local gateway**
- Country—Select <Country>, for example **United Kingdom**
- Owner—Select <Provider>, for example **UKprovider**
- Check the **Single Location Only check box**

Note If you enable "Single Location Only, the IOS device can be used in the selected location only.

- Select Location—Select the location to which you want to add local gateway, for example **Reseller_A: Customer_A: Division_A: 1402A2Loc2**

Step 5 Under **Connectivity Details**, enter the following:

- IP Address—<EthInterface IP Address>, for example **10.190.2.44**
- IP Address (alternate)—<Alternate IP Address>, for example **10.191.2.44**
- IP Domain—<Domain name>, for example **ipcbuemea.cisco.com**
- Config user Required—Select the check box if IOS config user is configured.

Note Config user required flag and config user name should be provided only if the IOS device is configured with telnet/ssh login name.

- Config User name—<IOSConfigUser>, for example **cisco**
- Config Password—Enter <IOS device config password>, for example **cisco**
- Enable Password—Enter <IOS device enable password>, for example **cisco**
- Software Version—Select the proper IOS version, for example, **IOSDevice: 15.x**

Step 6 Click **Finish**.

Define Local Gateways

To define the added IOS device in a Local Gateway do the following:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click on the newly added IOS device hyperlink

Step 3 Under **Device Roles**, Gateway, Click **Add**.

Step 4 Under **Gateway Details,** select the local gateway protocol, **H.225**

Step 5 Click **Next.**

Step 6 Under **Gateway Details > Select Device**, Select the CUCM cluster to which you want to register the gateway. For example, **IPPBX:e2c2p, Version 7.1.x**

Step 7 Click **Next.**

Step 8 Under **Gateway Functions**, check the **PSTN Local check box**.

Step 9 Click **Add.**

Repeat this for all required Local Gateways.

Configure Gateway Hardware

To configure gateway hardware do the following:

Step 1 Go to **Network > IOS Devices**.

Step 2 Click the IOS Device, for example **e2lgw1.**

Step 3 Under **Gateway Details**, Click the IOS Device, for example **e2lgw1.**

Step 4 Under **Interface Details**, Click **Gateway Hardware Configuration**.

Step 5 Under **Device Settings**, enter the following:

- Call Classification—<Call_Classification>, select **OFFNET**
- Packet Capture Mode—<PacCapMode>, for example, select **<None>**
- Gateway Voice Interface<Ehternet H.323 bind interface>, for example **FastEthernet0/0**
- Tunnelled Protocol—<TunnelledProtocol>, select **<None>**
- Signalling Port—<H323SigPort>, **1720**
- Media Resource Group List—select the MRGL, for example, **e2mrglClu2**

Step 6 Under **Call Routing Information - Inbound Calls**, enter the following:

- Significant Digits—< Significant Digits >, select **ALL**
- Calling Search Space—<InboundCSS>, select **Incoming Call to Local PSTN Gateway**

Step 7 Under **Call Routing Information - Outbound Calls**, enter the following:

- Calling Party Selection—Select **Originator**
- Calling Party Presentation—Select **Allowed**
- Redirecting Number IE Delivery - Outbound—Check the check box

Note Redirecting Number is required for all calls forwarded from HUCS to PSTN via local gateway. Hence, Redirecting Number IE Delivery flag must be set for the local gateway outbound calls.

Step 8 Click **Add.**

Define Local Gateway Interfaces

In Hosted UCS 7.1(a) Local Gateways can route calls via:

- PRI interfaces;
- BRI interfaces.

Following sections describe how different interfaces can be configured:

- Define Local Gateway PRI Interface
- Define Local Gateway BRI Interface

Note Ensure that the Country has been added to the Provider before adding a Local Gateway Interface.

Define Local Gateway PRI Interface

Two steps are required to define a Local Gateway PRI Interface. The administrator needs to define a Port used on the Local Gateway, and then define a trunk used on the previously defined port.

To define a PRI port used on the Local Gateway:

Step 1 Go to **Network > IOS Devices**.

Step 2 Click the IOS Device, for example **e2lgw1**

Step 3 Under **Gateway Details,** click the IOS device, for example **e2lgw1**

Step 4 Under **Interface Details**, click the **Gateway Hardware Configuration.**

Step 5 Click **Add Port.**

Step 6 Under **Add H.323 Port Summary,** enter the following:

- Port Type— <PortType>, select **E1** (for PRI)
- Port Number—<Slot/Subslot/Port>, for example **0 / 1 / 0**
- Add Range (optional)—<PortRange>, for example **0 / 1 / 1** (if you want to add multiple ports)

Step 7 Click **Add**.

To define a Trunk used on the previously defined Port:

Step 1 Go to **Network > IOS Devices**.

Step 2 Click the IOS Device, for example **e2lgw1.**

Step 3 Under **Gateway Details,** click the IOS device, for example **e2lgw1.**

Step 4 Under **H.323 Ports**, Select **E1** port you want to configure.

Step 5 Click **Configure Selected.**'

Step 6 Under **Port Configuration**, enter the following:

- Framing—<FramingMethod>, for example **NO-CRC4**
- Clock Source—<ClockSrc>, **line**
- Line Coding—**HDB3**

- ISDN Switch Type—<ISDNSwitchType>, for example, select **primary-net5**
- ISDN B Channel Number Order—select **descending**
- Set Calling Party NOA for Outgoing Calls—<ANOA>
- Set Called Party NOA for Outgoing Calls—<BNOA>

Note If the NOA check box is selected for both cgpn and cdpn, then cgpn & cdpn are set in a relevant format together with appropriate NOA based on the calling number and called destination; If the NOA check box is not selected for both cgpn and cdpn, then the NOA is set to Unknown. Both cgpn and cdpn are prefixed with appropriate leading digits to distinguish calling number and called destinations.

- Local Dialing Method—<LocalDialMethod>, select a local dialing method applicable for that location, for example **No Local dialing**

Note Local Dialing: This choice relates to the expected format of the cdpn (B) for outgoing/incoming PSTN calls. If there is no distinction between national and local dialing, or if the format of the number for local dialing should not be set, select **No local dialing**. All non-international calls will be treated as national calls. If the cdpn (B) for local calls needs to be presented to/from PSTN without an area code (for example some US locations allow 7-digit local dialing), select **Local dialing without area code**. In the US, some areas support 10-digit local dialing. In this case, select **10-digit local dialing**.

- National Area Code (for local dialing)—<NAC>, enter the NAC, for example **1402**

Note For any selected local dialing method, the National Area code must be entered.

Step 7 Click **Next >>**

Step 8 Ensure that all the configuration details entered are correct and then click **Add.**

When configuring a PRI/BRI trunk, the NOA selected for Cgpn and Cdpn does not get updated properly on the USM page and database. The NOA should be modified manually again to set it properly. To solve this issue, do the following:

Procedure:

Step 1 Go to **Gateway Hardware Configuration.**

Step 2 Select the port and click Configure Selected on the port; for example, **0/1/0.**

Note Ensure to configure the port by selecting the check box besides the port and clicking "Configure Selected". If you configure a port by clicking the hyperlink on the port number, it does not configure the gateway properly.

Step 3 Set NOA and other parameters properly.

Step 4 Cick Modify.

Step 5 Ensure that settings are properly reflected on the USM page.

Repeat this for all required PRI Interfaces and for all Local Gateways.

Define Local Gateway BRI Interface

Two steps are required to define a Local Gateway BRI Interface. The administrator needs to define a Port used on the Local Gateway, and then define a trunk used on the previously defined port.

To define a BRI port used on the Local Gateway:

Step 1 Go to **Network > IOS Devices**.

Step 2 Click the IOS Device, for example **e2lgw1.**

Step 3 Under the Gateway Details, click the IOS device, for example **e2lgw1.**

Step 4 Under **Inerface Details**, Click the **Gateway Hardware Configuration**.

Step 5 Click **Add Port**.

Step 6 Under **Add H323 Port Summary**, enter the following:

- Port Type—<PortType>, select **BRI**
- Port Number—<Slot/Subslot/Port>, for example **1 / 1 / 0**
- Add Range (optional)—<PortRange>, for example **1 / 1 / 1** (for adding multiple ports)

Step 7 Click **Add**.

To define a Trunk used on the previously defined Port:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click the IOS Device, for example **e2lgw1.**

Step 3 Under the Gateway Details, click the IOS device, for example **e2lgw1.**

Step 4 Under **Inerface Details**, Click the **Gateway Hardware Configuration**.

Step 5 Under H.323 Ports, Select **BRI** port.

Step 6 Click **Configure Selected.**'

Step 7 Under **Port Configuration**, enter the following:

- ISDN Switch Type—<ISDNSwitchType>, for example, select **basic-net5**
- ISDN Layer1 Emulate—<Port Side>, select **Network** (if the BRI port side is NT)
- ISDN Protocol Emulate—<ProtocolEmulation>, select **Network** (if the BRI port side is)
- ISDN Overlap Receiving—select **no**
- ISDN Twait-Disable—select **no**
- Set Calling Party NOA for Outgoing Calls—<ANOA>
- Set Called Party NOA for Outgoing Calls—<BNOA>

Note If the NOA check box is selected for both cgpn and cdpn, then cgpn & cdpn are set in a relevant format together with appropriate NOA based on the calling number and called destination. If the NOA check box is not selected for both cgpn and cdpn, then the NOA is set to Unknown. Both cgpn and cdpn are prefixed with appropriate leading digits to distinguish calling number and called destinations.

- Local Dialing Method—<LocalDialMethod>, select a local dialing method applicable for that location, for example **No Local dialing**

Note Local Dialing: This choice relates to the expected format of the cdpn (B) for outgoing/incoming PSTN calls. If there is no distinction between national and local dialing, or if the format of the number for local dialing should not be set, select No local dialing. All non-international calls will be treated as national calls. If the cdpn (B) for local calls needs to be presented to/from PSTN without an area code (for example some US locations allow 7-digit local dialing), select Local dialing without area code. In US, some areas support 10-digit local dialing. In this case, select 10-digit local dialing.

- National Area Code (for local dialing)—<NAC>, enter the NAC, for example **1402**

Note For any selected local dialing method, the National Area code must be entered.

Step 8 Click **Next >>**

Step 9 Ensure that all the configuration details entered are correct and then click **Add.**

When configuring a PRI/BRI trunk, the NOA selected for Cgpn and Cdpn does not get updated properly on the USM page and database. The NOA should be modified manually again to set it properly:

Procedure:

Step 1 Go to **Gateway Hardware Configuration.**

Step 2 Select the port and click the Configure Selected of the port, for example, **1/1/0.**

Note Ensure to configure the port by selecting the check box besides the port and clicking "Configure Selected". If you configure a port by clicking the hyperlink on the port number, it does not configure the gateway properly.

Step 3 Set **NOA and other parameters** properly and click **Modify**.

Step 4 Ensure that settings are properly reflected on the USM page.

Repeat this for all required BRI Interfaces and for all Local Gateways.

Add E.164 inventory for local gateway location

In this section, E.164 numbers which should be associated with local gateway location are added in ranges of 1, 10, 100, 1000, 10000, (10^x where x= 0,1,2,3,4) as local breakout E.164 numbers.

Please refer Adding Area Codes, page 4-3, for creating E164 inventory

Note The E164 numbers for local gateway location should be added as "Local" break out numbers.

Move E.164 numbers to Local Gateway Location

Refer Moving E.164 Number Inventory, page 4-13.

Location Administration

This section describes the steps required to configure various location parameters, which are specific for Local PSTN breakout support, for example changing the location preferences.

Note Before proceeding with the provisioning steps in this section ensure that:

- A local gateway location is added with Internal numbers
- E164 number inventory is added and moved to local gateway location
- You haven't assigned any range of E164 numbers to internal numbers.

For further details refer to Section 8 and 13 on "Hosted UCS 7.1(a) Release - USM Provisioning Guide.

This section has the following topics:

Caution Ensure that you are administering the correct Location. The name of the Location will be shown on the screen

Change Location Preference

To change location preference do the following:

Step 1 Go to **General Administration > Locations**.

Step 2 Select the location you want to configure.

Step 3 Click **Preferences.**

Step 4 Click **AssociateFNNinRanges.**

Step 5 In **Location > AssociateFNNinRanges,** Check the available Check box.

Step 6 Click **Modify**.

Activate Local Gateway Port

To activate a local gateway port on a location, do the following:

Step 1 Go to **General Administration > Locations.**

Step 2 Select the location you want to activate port.

Step 3 Go to **Location Administration > Telephony > Gateways.**

Step 4 Select the gateway port to activate, for example Port **1/0/0**

Step 5 Click **Activate**.
An **Advanced Dial Plan Configuration page** is displayed.

Step 6 Select the Call of Service—**Incoming Calls to Local PSTN Gateway.**

Step 7 Click **Activate.**

Note When there is a dial plan active for the location, the user can select additional ports or additional gateways from the deactivated port section and select the Activate button. This will take the user to the Advanced Dial Plan Configuration page.

Note When adding ports, the user is restricted from changing the Class of service and the device priority of existing H.323/H.225 protocol ports.

Apply Local Gateway Call Routing

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 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 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 with 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.

To enable location level call routing, follow the steps below:

Step 1 Go to **General Administration > Locations**.

Step 2 Select the location in which port is activated.

Step 3 Go to **Location Administration > Telephony > Gateways > Call Routing.**

Step 4 Select the Call Types which you want to apply on local gateway. For example, Select **All Local.**

Step 5 Click **Submit.**

Step 6 Go to **Location Administration > Telephony > Gateways > Call Routing.**

Step 7 Under **Local Gateway Port Call Routing**, select **all call types.**

Step 8 From **Apply Call Routing Configuration to Trunks** menu, select **Once for all the Call Types.**

Step 9 Click **Submit.**

Note The Local Gateway Port Call Routing section is displayed on the screen once the location level call routing has been applied and H.323 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:

- Once for all the Call Types (default) - This implies that call routing configuration will be applied to trunks once for all the call types
- Once per Call Type - 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.

Assign Range of E.164 Numbers to Internal Numbers

For a range of internal extensions, USM administrator can assign a range of E.164 numbers to an IP Phone, so that users can receive calls from the PSTN on these extensions. For locations with Local PSTN breakout support, E.164 numbers are associated with internal numbers by associating a range of 10^n numbers, where ‘n’ can be selected from the values {0,1,2,3,4}.

Ensure that the Location preference 'AssociateFNNinRanges' has been enabled. To assign a range of E.164 numbers to internal numbers using the in-ranges option, do the following:

Step 1 Go to **Location Administration > External Numbers.**

Step 2 Click **Associate Range.**

Step 3 Under **Select the Size of Range,** enter the following:

- Range Size—<RangeSize>, for example **10**.
- Click **Next >>**

Step 4 Under **Details**, enter the following for the Range:

- PSTN Number range—<PSTNRange>, for example **2122110200-2122110209**
- Extension Number range—<ExtRange>, for example **0200-0209**

Step 5 Click **Submit**.

Note In order to associate a range of numbers not equal to 10^n numbers, where ‘n’ can be selected from the values {0,1,2,3,4}, the second step needs to be repeated a few times. For example, if a range of 21 numbers needs to be associated, this step needs to be repeated three times ($2 * 10^1 + 1 * 10^0$).

Note Starting from Hosted UCS 6.1(a), USM invokes the PGW TimesTen driver and uses the TimesTen Input in the AssocaiteFNN transaction (AssociateFNN and AssociateFNNLocalGW scripts) of the PGW_TimesTen_Any model worksheet to create an import file and transfer it to the PGW, where it invokes the HUCSprovx10 PGW script and inserts the associations into the PGW TimesTen database.

Repeat this multiple times (if the range is not equal to 10^n numbers, where n can be selected from the values {0,1,2,3,4},) and for all required locations.

Add Location PSTN published number

To add a PSTN published number for a location, refer the Section Adding PSTN Published Numbers, page 4-15.

Add Location Emergency Published Number

To add an emergency published number for a location, refer the section Adding Emergency Published Numbers, page 4-15.

After the local gateway is provisioned, enter the following IOS commands on the gateway in configuration mode.

```
voice service voip
fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
modem passthrough nse codec g711ulaw
allow-connections h323 to h323
h323
emptycapability
h245 passthru tcsnonstd-passthru
```

Modify/Delete Local Gateway Port Call Routing

Note The steps mentioned in this section are only for modifying or deleting the existing local gateway port call routing and it should be performed if you want to modify/delete the provisioned local gateway, otherwise not required.

To Modify/Delete location level call types, follow the steps below:

Step 1 Go to **General Administration > Locations**.

Step 2 Select the location in which port is activated.

Step 3 Go to **Location Administration > Telephony > Gateways > Call Routing.**

Step 4 Under **Local Gateway Port Call Routing**, select applicable call types which you want to modify / delete.

Step 5 Click **Modify,** if you would like to modify the call routing types or click **Delete** to remove the local gateway call routing for all the call types.

Modify/Delete Location Call Routing

Note The steps mentioned in this section are only for modifying or deleting the existing location call routing and it should be performed if you want to modify/delete the provisioned local gateway otherwise not required. Ensure that the steps in Modify/Delete Local Gateway Port Call Routing, page 7-21 is already done before proceeding with this section

To Modify/Delete location level call routing, follow the steps below:

Step 1 Go to **General Administration > Locations.**

Step 2 Select the location in which port is activated.

Step 3 Go to **Location Administration > Telephony > Gateways > Call Routing.**

Step 4 Under **Location Call Routing**, select applicable call types which you want to modify/delete.

Step 5 Click **Modify,** if you would like to modify the call routing or click **Delete** to remove the location call routing.

Modify/Delete Local Gateway Dial Plan

Note The steps mentioned in this section are only for modifying or deleting the existing location dial plan and it should be performed if you want to modify/delete the provisioned local gateway otherwise not required. Also, ensure that the steps in Modify/Delete Local Gateway Port Call Routing, page 7-21 and Modify/Delete Location Call Routing, page 7-21 are already done before proceeding with this section.

To Modify/Delete location dial plan, follow the steps below:

Step 1 Go to **General Administration > Locations**.

Step 2 Select the location in which port is activated.

Step 3 Go to **Location Administration > Telephony > Gateways.**

Step 4 Click **Modify Dial Plan**, if you would like to modify the dial plan Class of Service or click **Delete Dial Plan**, to remove the local gateway dial plan.

Note If you would like to change the PRI/BRI trunk definitions of the local gateway, then the location level gateway configurations on USM should be removed as in Modify/Delete Local Gateway Port Call Routing, page 7-21, Modify/Delete Location Call Routing, page 7-21 and Modify/Delete Local Gateway Dial Plan, page 7-22. Otherwise the USM administrator would not allow to modify some of the fields of trunk definition.

Voicemail Retrieval via Location Local Breakout

In HUCS7.1a release, it is possible to configure the Hosted UCS components so that users can retrieve their Voicemail via the LGW.

In addition to this it is possible to configure multiple E.164 numbers for Voicemail retrieval via LGW in order to allow users in different locations to retrieve Voicemails via the closest LGW.

To configure E.164 numbers for voice mail pilot number in order to retrieve voice mail via local gateway PSTN, follow the steps below:

Step 1 Go to **General Administration > Locations.**

Step 2 Select the location in which both local gateway and voicemail service are available.

Step 3 Click **Advanced Management.**

Step 4 Click **Voicemail Mgt**. You should see the available "Local" breakout PSTN numbers. If there is no PSTN numbers available in that location, add local break out E.164 numbers) and move it to this location.

Step 5 Click **Associate Range**

Step 6 Select the Range Size (1, 10, 1000, 10000) based on the total E.164 numbers which you want to associate to a voice mail pilot., for example, select **1**

Step 7 Under **Map a PSTN Range to a single extension**, select the PSTN Number Range for the selected Extension Number (VM pilot number), for example, **01637111010 - 01637111010**.

Step 8 Click **Submit.**

CHAPTER 8

Provisioning LBO Location with Cisco Emergency Responder

This chapter explains the deployment of Cisco Emergency Responder (CER) in the HUCS 7.1A platform. This chapter has the following sections.

Prerequisites for Deployment of CER

Before deploying CER the System Integrator should obtain the following minimum information:

- PRI trunks to connect to the service provider.

Note In Hosted UCS 7.1A CAMA trunks cannot be configured.

- Default emergency response location (ERL) automatic location informaiton (ALI) data and emergency location identification number (ELIN).
  - ELIN(s) Direct Inward Dial (DID) numbers for use as emergency location identification numbers (ELIN), for the emergency response locations (ERL).
  - ALI Data for the ERL. Emergency calls are routed to the appropriate PSAP based on the ELIN of the emergency caller. To route the call, the telephony network must have your automatic location information (ALI) that maps these ELINs to a location and also supplies the location information that appears on the PSAPs screens to help them locate the caller.
- ERL and associated ELIN(s) for each location. For every location that is going to be provisioned to use CER, ensure that you have the ELIN (DDIs) and ALI data.

Static, Basic and Repetitive configuration

While most of the provisioning is run once for the deployment of a CER group, some will need to be run once every time a new customer, location, phone switch, phone, ERL or ELIN is added to the platform.

Note One customer location as defined by the BVSM does not necessarily translate to one Emergency Response Locations (ERL).

The following steps must be run to add the switch / phone to the CER:

Step 1 LAN Switch SNMP configuration (new switch).

Step 2 Add the SNMP and related network IP data to the CER (new switch).

Step 3 Select poll switch to get latest phone information (new switch / phone).

Step 4 Phones discovered must be tagged to their respective ERL(s). (new switch / phone).

Another repetitive task is running the PSAP callback section when adding a new customer.

Note For further details on Planning for CER, refer to:

http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911plan.html

Static Configuration

This section has the following topics:

- Configure a CER server group, page 8-2
- Cisco Unified CM Static Configuration, page 8-3
- LAN Switch SNMP / CDP Configuration, page 8-4
- Add SNMP and related network data to CER, page 8-4
- CER to Identify and Poll the LAN Switches, page 8-5

Configure a CER server group

In CER, Log in to the Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin**.**

Step 1 Select **System > Cisco ER Group Settings.**

Step 2 Fill in the group settings. Many fields have defaults that should work for most networks. At minimum, you must configure these fields:

- Cisco ER Group Name—Enter a name for the group. for example **CERGroup1**

- Peer TCP Por—<PeerTCPPort>, for example **17001**
- Heartbeat Count—<HeartbeatCount>, for example **3**
- Heartbeat Interval (secs)—<HeartbeatInterval>, for example **30**
- Active Call Timeout (mins)—<ActiveCallTimeout>, for example **180**
- Calling Party Modification—Select **Disable,** from the drop-down menu

Step 3 Click **Update Settings**.

Cisco Unified CM Static Configuration

When you configure the SNMP strings for the switches, you must also configure the SNMP strings for the Cisco Unified CM servers. CER must be able to make SNMP queries of all Cisco Unified Communication Manager servers in the cluster that it supports.

In Unified Communication Manager, to configure the SNMP strings on CCM, log into the Serviceability page:

https://<Unified_CM_IP_Address_or_name>/ccmservice.

Choose **SNMP > V1/V2c > Community String**, and configure the following:

Step 1 From the Server drop-down list box, choose the server for which you want to configure a community string, for example **10.10.4.2.**

Step 2 Click **Add New**.

Step 3 In the Community String Name field, enter a name for the community string, for example **CERGroup1**.

Step 4 From the **Host IP Addresses Information group box**, click the **Accept SNMP Packets only.**

Step 5 In the **Host IP Address field**, enter the IP addresses of the Primary Cisco ER server, for example **10.10.9.10.**

Step 6 Click **Insert**.

Step 7 If the Backup Cisco ER Server is installed, repeat this process.

Step 8 From the **Access Privileges** drop-down list box, choose the **ReadOnly access level.**

Step 9 Check the **Apply To ALL Nodes** check box, to apply the community string to all nodes in the cluster.

Step 10 Click **Save.**
The message, "Changes will not take effect until you restart the SNMP master agent. To restart the SNMP master agent service, click OK", is displayed.

Note Repeat the above steps to ensure that all the servers in the CUCM cluster have a community string, as CER must be able to make SNMP queries of all Cisco Unified Communication Manager servers in the cluster that it supports.

LAN Switch SNMP / CDP Configuration

CER uses Cisco Discovery Protocol (CDP) to locate phones, so you should enable CDP on all of your switches. If you do not enable CDP, CER must use the Content Addressable Memory (CAM) table on the switch to track phones which is less efficient than using CDP.

CER also uses SNMP to obtain information about the ports on a switch. CER only reads SNMP information; it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

On the Phone Switch, to enable CDP and to configure the SNMP read community string, enter the following commands in Global Configuration mode:

```
cdp run
snmp-server community <Community_String> RO
```

For example:

```
hostname(config)#cdp run
hostname(config)#snmp-server community CERGroup1 RO
```

Add SNMP and related network data to CER

The Cisco Emergency Responder uses SNMP to obtain information about the phone ports on a switch. Obtain the read community strings from all of the switches to be defined in the CER.

In Cisco Emergency Responder, to configure the SNMP connection, log in to the Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin.

Step 1 Choose **Phone Tracking > SNMP Settings.**

Step 2 On the SNMP Settings page, enter the following:

- Enter IP address pattern to which you want to associate an SNMP read community string.

Note If all of your switches use the same read community string, enter *.*.*.*. If subsets of your switches use the same strings, create a mask that covers those subsets. If you use a separate string for each switch, you must enter each switch on this page.

Enter the timeout and retries values. The suggested optimal values are **10 - 15** seconds for timeout, and **2 - 3** for retries.

- Enter the read community string, for example **CERGroup11**.

Step 3 Click **Insert.**

Note Note: If your CER servers, Cisco Unified CM servers, and Cisco IP Phones are located in a different subnet than your switches, you must either configure the subnets for the Cisco Unified CM server, phones and the subnet for the switches OR use *.*.*.*.

CER to Identify and Poll the LAN Switches

You must inform CER the switches to be managed. CER tracks port changes, including changes to the devices connected to those ports, and can recognize which ports have phones connected to them. Identify all switches that might have phones attached to them, essentially all edge switches.

After creating the initial switch list on CER, make mass changes to switch definitions by exporting the switch definitions, editing the export file, and re-importing the file.

Note Ensure that you configure the SNMP read community strings before adding switches.

In Cisco Emergency Responder, to configure the LAN Switch log into the CER Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin.

Step 1 Choose **Phone Tracking > LAN Switch Details**.

Step 2 On the **LAN Switch Details** page, enter the following:

- Enter the IP address or DNS name of the switch—for example **10.10.20.1**
- Enter the Description—for example Phone Switch: **PH-SW01**

Step 3 Click **Insert** to add the switch to the CER configuration.

Note If CER prompts the message “Do you want to run the switch-port and phone update process”, then run this process. However, if you are adding more than one switch, you can skip running the process until you add the last switch and then re-run by selecting **Phone Tracking > Run Switch-Port & Phone Update**, at a later point in time when all the phones have been plugged into the phone switch.

Provisioning CER

This section contains the following topics:

Define Cisco ER Groups in VOSS-USM

To define a Cisco ER Group in VOSS-USM, do the following:

Step 1 Go to **Network > Emergency Responder.**

Step 2 Click **Add.**

Step 3 Click **Add** corresponding to CiscoEmergencyResponder in the Product Selection screen.

Step 4 Under **CERGroup Details**, enter the following:

- CERGroup Name: <uniquename>, same as the Cisco ER Group Name configured in Cisco ER, for example **CERGroup1**
- CERGroup Description: <CERGroupdescription>, for example **Cisco ER Group 1**
- ELIN for Default ERL: <ELINDefaultERL>, for example **4085550001**

Note The Default ERL's ELIN should belong to the Service Provider Representative Location and should be the DID of the phone number of Service Provider Representative.

- Peer TCP Port: <PeerTCPPort>, for example **17001**
- Heartbeat Count: <HeartbeatCount>, for example **3**
- Heartbeat Interval (secs): <HeartbeatInterval>, for example **30**
- Active Call Timeout (mins): <ActiveCallTimeout>, for example **180**
- UDP Port Begin: <UDPPortBegin>, for example **32000**
- Software Version: <CERVersion>, **CiscoEmergencyResponder : Any**
- Check the **Detailed trace file of configuration sessions?** check box
- Uncheck **Encrypt configuration sessions?** check box
- Click **Next**

Step 5 Under **Primary Cisco Emergency Responder Details**, enter the following:

- Host Name: <PrimaryCERHostName>, for example: **CER1a**
- Description: <PrimaryCERDescription>, for example: **Primary Cisco ER Server**
- IP Address: <PrimaryCERIPAddress>, for example: **10.10.9.10**
- Config User Id: <CERSystemAdmin>, for example: **CERAdministrator** (The user should be part of the CER System Administrator user group)
- Config Password: <CERSystemAdminPassword>, for example: **cisco123**
- Route Point for Main Server: <RPforMainServer>, for example: **911**

Under **Backup Cisco Emergency Responder Details**, enter the following:
(optional)

- Host Name: <SecondaryCERHostName>, for example: **CER1b**
- Description: <SecondaryCERDescription>, for example: **Secondary Cisco ER Server**
- IP Address: <SecondaryCERIPAddress>, for example **10.10.9.11**
- Config User Id: <CERSystemAdmin>, for example **CERAdministrator** (The user should be part of the CER System Administrator user group).
- Config Password: <CERSystemAdminPassword>, for example **cisco123**
- Route Point for Backup Server: <RPforMainServer>, for example **912**

Step 6 Click **Add.**

Associate CER Groups with CUCM Clusters in VOSS-USM

To associate a Cisco ER Group with a Unified CM cluster in VOSS-USM do the following:

Step 1 Go to **Network > Emergency Responder**

Step 2 Click Connectivity corresponding to the Cisco ER Group, for example: **CERGroup1.**

Step 3 Click **Emergency Responder > PBX,** in the Connectivity Management Screen.

Step 4 Select the Unified CM cluster, for example **CUCM-POP1.**

Step 5 Click **Connect.**

Step 6 Under **Emergency Responder Details**, enter the following:

- Telephony Port Begin Address: <PortBeginAddress>, the number of the first CTI port to use for calling onsite alert (security) personnel, for example **3001**
- Number of Telephony ports: <NumberofPorts>, Number of CTI Ports, for example **10**

Note Ensure that the CTI Port numbers do not overlap with other configured Directory numbers, Extensions, as they are non-dialable, for example **3001-3010**.

Step 7 Click **Connect.**

Create User and associate with CTI Ports and Route Points in CUCM

In Cisco Unified Communication Manager, to create a Cisco Emergency Responder Cisco Unified Communication Manager user do the following:

Step 1 Log into the Cisco Unified CM Administration page: https://<Unified_CM_IP_Address_or_name>/ccmadmin,

Step 2 Choose **User Management > Application User**.

Step 3 Click **Add New** and configure the following:

- User ID: <UserID>, for example CERUser
- Password; <Password>, for example cisco123
- Confirm Password: <Password>, re-enter the password, for example cisco123

Step 4 In the **Device Information section**, select the configured Cisco ER route point(s) and CTI port(s), for example route points **RP911, RP912, RPELIN913**, and CTI Ports **3001-3010** and then click the down arrow to add the selected devices to the user's control list.
The list of devices appears in the Controlled Devices area.

Step 5 Click **Save.**

Step 6 Choose **User Management > User Group**, and configure the following:

Step 7 Click the **Standard CTI Enabled** user group link to display the User Group configuration page.

Step 8 Click **Find** to get a listing of users.

Step 9 Check the checkbox corresponding to the created user ID, for example **CERUser**

Step 10 Click **Add Application Users to Group.**
Cisco Unified Communications Manager adds the selected user to the Standard CTI Enabled user group.

Repeat the above procedure to add the Standard CTI Allow Calling Number Modification group to the CERUser.

Add CUCM data in CER

Note VOSS-USM cannot provision the CER; therefore you have to manually associate the CER with the CUCM cluster, define the CUCM user and the CTI devices that user will control.

In Cisco ER, to define the Unified CM cluster on Cisco ER do the following:

Step 1 Log into the CERAdministration page:
https://<Cisco_ER_IP_Address_or_name>/ceradmin.

Step 2 Choose **Phone Tracking > Cisco Unified Communications Manager**.

Step 3 In the **Cisco Unified Communications Manager page**, enter the following:

- Cisco Unified Communications Manager: <CUCMName>, IP address or DNS name of the server, for example **10.10.4.2**.

  Note This server must be running CCM and SNMP services. Do not define more than one CCM server within the same CCM cluster in the CER configuration.

- CTI Manager: <CTIManagerIP>, IP address or DNS name of the CTI manager for the cluster to which the server belongs, for example **10.10.4.2** (Unified CM Subscriber in primary POP)
- CTI Manager User Name: <CERCUCMUser>, for example **CERUser**. (created earlier)
- CTI Manager Password: <CTIManPass>, for example **cisco123** (created earlier)
- Backup CTI 1 Manager: <BackupCTI1manager>, IP address or DNS name of the first backup CTI manager for the cluster, for example **10.10.4.3** (Unified CM Subscriber in secondary POP).
- Backup CTI 2Manager: <BackupCTI2Manager>, IP address or DNS name of the second backup CTI manager for the cluster
- Telephony Port Begin Address: <PortBeginAddress>, the first CTI port address in the sequence of ports created for Cisco ER, for example **3001**
- Number of Telephony Ports: <NumberofPorts>, the number of CTI ports in the sequence you created for Cisco ER's use, for example **10**
- Onsite Alert Prompt Repeat Count-The number of times a prompt is given on the onsite security phone. for example, **2**

Step 4 Click **Insert** to add the Unified CM to the Cisco ER configuration.
Cisco ER adds the Cisco Unified CM server to the list of servers.

Configure the Default ERL and ELIN on CER

Calls from the default ERL are managed by an IP Phone located within the HUCS platform. The HUCS service provider creates a Customer & Location and a dedicated phone at that location, using VOSS-USM as per the generic HUCS provisioning guide.

This section contains the following topics:

Setup onsite alert support for Default ERL

It is recommended that for every ERL at least one onsite security personnel is identified and assigned to the ERL. If an emergency call is made from an ERL, the associated onsite alert personnel receives a telephone call indicating that an emergency call is made. The personnel ID created in this step will be associated with an ERL as detailed in the following section:

For the Default ERL make sure that the Onsite Alert Number is the Service Provider Representative number, as the Default ERL is non-multi tenantable and caters to all the Customer/Location provisioned to use CER.

Note This step is repeated whenever a new onsite personnel has to be added to the Default ERL.

Step 1 In Cisco ER, log into the CER Administration page:
https://<Cisco_ER_IP_Address_or_name>/ceradmin:

Step 2 Select **ERL > Onsite Alert Settings**.
Cisco ER opens the Onsite Alert Settings page.

Step 3 Enter the unique ID, name, telephone number of a security or onsite alert person.

Note The telephone number should be entered as a FINT (CPID+RID+SLC+EXT).

Step 4 Use the following available settings:

- CPID—Available on the CCM Cluster Management Page of the PBX Device menu on USM
- RID Code—Available on the Manage Location page of the Location menu on USM
- SLC—Available on the Manage Location page of the Location menu on USM
- Extension (Ext)—Available directly from the phone
- Click **Insert**.

Note CER adds the person to the list of onsite personnel. Repeat until you define all security or onsite personnel.

For further details on Setting up onsite alert support, please go to the following section of the CERAdministration Guide:

http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911conf.html#wpxref64756

Create Default ERL and ELIN

This step creates the Default ERL and uses the Default ELIN for the CER group. In a live deployment this step should be done only after a valid ERL, ELIN and data for the ALI database is available.

Note PSAP Callback is not supported for the Default ERL. The callback from the PSAP with default ERL will be sent to the Service Provider Representative, as the ELIN for the default ERL is the DID of the Service Provider Representative's DN.

The Default ERL is used internally by CER only if no other ERL is configured for a phone. The Default ERL should not be configured for any of the Switch Ports, Unallocated Phones, Manually Configured Phones or IP Subnets. CER uses the Default ERL for all emergency calls when the CER server is first started (or restarted when there is no standby CER server), until the initial switch port update is finished.

It is recommended that a phone / line at a dedicated location belonging to the service provider be used as Onsite Alert for the Default ERL so as to receive calls that are directed to the default ELIN.

Procedure:

Step 1 Choose **ERL > Conventional ERL**.
CER opens the Find and List ERLs page.

Step 2 Click **Configure Default ERL**.
CER opens the ERL Information for Default window.

Step 3 In the **ERL Information for Default** window, configure the following in the ELIN Settings section:

- Route/Translation Pattern—<RTPDefaultERL>, Route Pattern for the Default ERL configured in Cisco Unified CM.
  - To identify the route pattern, log into the Cisco Unified CM Administration page: **https://<Unified_CM_IP_Address_or_name>/ccmadmin.**
  - Choose **Call Routing > Route/Hunt > Route Pattern**.
  - Select **ends with** as the search pattern.
  - Add **911** to the search box and click **Find**. This Route Pattern should be used in CER, for example: **29999999999.911**
- ELIN: <ELINDefaultERL>, for example **4085550001** (The Elin should be a DID number from the Service Provider Representative's Location)
- Onsite Alert Settings—Highlight the available IDs under Available Onsite Alert IDs

Step 4 Click Add

Step 5 Add ALI data.

For detailed information refer URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911page.html#wp1009232

Modify Default Route Pattern on the CUCM

In Cisco Unified CM, to create a Cisco ER Cisco Unified CM user do the following:

Step 1 Log into the Cisco Unified CM Administration page: **https://<Unified_CM_IP_Address_or_name>/ccmadmin**

Step 2 Choose Ca**ll Routing > Route/Hunt > Route Pattern.**

Step 3 Select **ends with** as the search pattern.

Step 4 Add **911** to the search box and click **Find**.

Step 5 Click the **Route Pattern**, for example: **29999999999.911**

Step 6 Under the **Calling Party Transformations,** modify the following

- Calling Party Tranformation mask—Change the value of this field to the FINT of the Default ELIN (CPID + RID + 8 + SLC+ EXT)

Step 7 Under the **Called Party Transformations,** modify the following

- Called Party Transform Mask—Change the value in this field by entering the internal number (8 + SLC + EXT) of the Service Provider Representative
- Prefix Digits (Outgoing Calls)—Modify this field by deleting the contents, if any, of this field

Step 8 Click **Save**.

Add Cisco ER partition to the IncomingToCluster CSS

VOSS-USM cannot add additional partitions to an existing CSS. The created CER partition (for example EUSA) should be manually added to the IncomingToCluster CSS.

Caution This step is run once after the CER is being provsioned for the first time on a CUCM Cluster.

In Unified CM, to add the created CER partition (for example EUSA), to the IncomingToCluster CSS do the following:

Step 1 Log into the Cisco Unified CM Administration page: **https://<Unified_CM_IP_Address_or_name>/ccmadmin**.

Step 2 Choose **Call Routing > Class of Control > Calling Search Space.**

Step 3 Click **Find** and select the **IncomingToCluster** CSS.

Step 4 Choose the created CER partition (for example **EUSA**) in the **Available Partitions list** box and add it to the Selected Partitions list box by clicking the **arrow button** between the two list boxes.

Step 5 Click **Save.**

Repeat this for all required Unified CMs you want to connect to this CER Group, and for all required CER Groups.

Per-customer PSAP Callback Configuration

For each customer the administrator should provision a 913XXXXXXXXXX DN associated to a RPELIN913 CTI Route Point. This has to be done manually on unified CM in the Hosted UCS 7.1A lite release.

To find the Customer ID in VOSS-USM, do the following:

Step 1 Go to **General Administration > Customers.**

Step 2 Select the Customer for which you want to use Cisco ER for Emergency Handling, for example: **Customer1**

Step 3 Click **Advanced Mgt.**

Step 4 Customer Identified should be available on the next screen, for example: **Customer Identifier - 1**

In Cisco Unified CM, to create the 913XXXXXXXXXX DN associated to a RPELIN913 CTI Route Point, do the following:

Step 1 Log into the Cisco Unified CM Administration page: **https://<Unified_CM_IP_Address_or_name>/ccmadmin**

Step 2 Choose **Device > CTI Route Point**, search for the **RPELIN913** CTI Route Point

Step 3 Select the **RPELIN913** CTI Route Point (if some customers have already been provisioned to use Cisco ER for Emergency handling, you will see multiple **RPEILN913** CTI Route Points). Select any one of them for the next step).

Step 4 Add **new DN.**

- When configuring the platform for the first customer using CER a DN "913XXXXXXXXXX" would have be created by default and hence we do not have to create another one.
- For the second customer onwards you have to add a new DN (select the first available line), for example **Line [2] - Add a new DN**

Step 5 In the Directory Number Information section, configure the Directory Number with **913XXXXXXXXXX.**

Step 6 In the Directory Number Information section, first configure the **Route Partition** by selecting an entry from the drop down box with E#ISO# (where #ISO# is the ISO 3166-1 alpha-3 3-digit country code), for example **EUSA**.

Step 7 Click anywhere else on the screen to update the configuration. This step is used to auto-populate some of the other fields on the line and associate the line with the **RPELIN913 CTI** Route Point.

Step 8 Under Directory Number Settings, configure the Calling Search Space with EmergencyCust<CustomerID>, for example **EmergencyCust3** (Customer Identifier is retreived from VOSS-USM in the previous step).

Step 9 In the Directory Number Information section, change the Route Partition to EmergencyCust<CustomerID>, for example **EmergencyCust3**.

Step 10 Click **Save.**

Step 11 Choose **Device > CTI Route Point**, search for the **RPELIN913** CTI Route Point and check if **RPELIN913** CTI Route Points (with the associated **913XXXXXXXXXX** extensions) are registered. If this is not the case, proceed to the next step.

Step 12 Choose **User Management > Application User**, search for the Cisco ER Cisco Unified CM user, for example **CERUser.**

Step 13 Select the Cisco ER Cisco Unified CM user

Step 14 In the Device Information section, select the configured **RPELIN913** CTI Route Point from the **Controlled Devices** area and then click the **up arrow** to remove it temporarily from this area.

Step 15 Click **Save.**

Step 16 In the Device Information section, select the configured **RPELIN913** CTI Route Point from the Available Devices area and then click the **down arrow** to add the selected devices to the user's control list. The list of devices appears in the Controlled Devices area

Step 17 Click **Save.**

Step 18 Choose **Device > CTI Route Poin**t, search for the **RPELIN913** CTI Route Point and verify that all **RPELIN913** CTI Route Points (with the associated **913XXXXXXXXXX** extensions) are registered

Create Hardware Group with CER

BVSM uses Hardware Groups to determine which Network Components should be provisioned when; for example, an ELIN is is added to an ERL. To add a Hardware Group, use the following steps:

Step 1 Choose **Network > Hardware Groups.**

Step 2 Click **Add.**

Step 3 Under **Hardware Group Details,** enter the following:

- Name—<uniquename>; for example **cergr1-pgw4-e4c4-hwgrp**
- Description—<hwgrpdesc>, for example **City 4 CER Group 1-PGW 4-Unified CM Cluster 4**
- Limit usage of this Hard ware Group to—Any Action

Step 4 Under **Available Emergency Responder Servers,** choose the required Cisco ER Group, for example **CERGroup1**.

Step 5 Under **Available Transit Switches**, choose the required PGW, for example **PGW-ENT4.**

Step 6 Under **Available PBX Systems**, choose the required Unified CM Cluster, for example **e4c4.**

Add Location (with Enhanced Emergency Support)

To add Location, refer the VOSS deployment Guide.

While adding Location which needs to have CER support, make sure to check the **Enhancement Emergency Support** check box.

When a location that does not require Enhanced Emergency Support is created, add two site specific route patterns (911 and 9.911) to Unified CM to detect emergency calls, and tag the Calling Party Number with an Emergency call type (CT 4). This enables the PGW to detect emergency calls and handle them differently.

If Enhanced Emergency Support is selected when a location is created, instead of the two route patterns described above, add two site specific translation patterns (911 and 9.911) to Unified CM for detecting emergency calls and route them to Cisco ER.

Adding an ERL and ELIN for a location

This section creates a ERL and uses ELIN(s) provided for this ERL. The following topics are described in this section:

- Setup onsite alert support for Conventional ERL, page 8-14
- Add Emergency Response Location on VOSS-USM, page 8-15
- Add ELIN to ERL on the VOSS-USM, page 8-15

Setup onsite alert support for Conventional ERL

It is recommended that for every ERL at least one onsite security personnel is identified so that they can be assigned to ERLs such that If an emergency call is made from an ERL, the associated onsite alert personnel receive a telephone call indicating that an emergency call is made. The personnel ID created in this step will be associated with an ERL as detailed in the following section

Note This step needs to be repeated whenever a new onsite personnel has to be added to the Conventional ERL.

Procedure:

Step 1 In Cisco ER, log into the CER Administration page: **https://<Cisco_ER_IP_Address_or_name>/ceradmin**.

Step 2 Select ERL > Onsite Alert Settings.
Cisco ER opens the Onsite Alert Settings page.

Step 3 Enter the unique ID, name, telephone number of a security or onsite alert person.

Step 4 Use the following settings:

- Telephone number—Enter as a FINT (CPID+RID+SLC+EXT).
- CPID—Available on the CCM Cluster Management Page of the PBX Device menu on USM
- RID Code—Available on the Manage Location page of the Location menu on USM
- SLC—Available on the Manage Location page of the Location menu on USM
- Extension (Ext)—Available directly from the phone

Step 5 Click **Insert.**

Note CER adds the person to the list of onsite personnel. Repeat until you define all security or onsite personnel.

For further details on Setting up onsite alert support, please go to the following section of the CERAdministration Guide:

http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911conf.html#wpxref64756

Add Emergency Response Location on VOSS-USM

Depending on the requirements, a number of Emergency Response Locations (ERLs) can be associated to a location. For each of the created ERLs a number of ELINs can be defined.

To add an ERL in VOSS-USM, do the following :

Step 1 Go to **Location Administration > Telephony**.

Step 2 Click **Emergency Response Location Management.**

Step 3 Click **Add**.

Step 4 Under **Details**, enter the following:

- Name—<ERLName>, for example E-ERL1
- Description—<ERLDescription>, for example ELOC1-ERL1 Emergency Response Location 1
- Emergency Responder Hardware Group—<ERHwGroup>, for example ccm-pgw-cer-hwgrp

Click **Submit.**

Add ELIN to ERL on the VOSS-USM

For each of the created ERLs a number of ELINs can be defined.

To add an ELIN in VOSS-USM, do the following:

Step 1 Go to **Location Administration > Telephony**.

Step 2 Click **Emergency Response Location Management**.

Step 3 Select an ERL you want to add an ELIN to, for example **ELOC1-ERL1.**

Step 4 Click **Add ELIN**

Step 5 Select a DDI for the ELIN from the drop-down menu, for example **4085550008**

Step 6 Click **Submit.**

VOSS-USM cannot configure CER and therefore you must configure the ERL and ELINs manually.

In VOSS-USM, the information you provide should correspond with the information in VOSS-USM. To get this information from VOSS-USM:

Step 1 Go to **Location Administration > Telephony**.

Step 2 Click **Emergency Response Location Management**

Step 3 Select the ERL you want to configure, for example **ELOC1-ERL1**

Step 4 Use the following settings in the **Emergency Line Identification Numbers (ELINs)**:

- Line Number— <ELINNumber>, for example **408-5550008**
- Route Number— <RoutePattern>, for example **408-5550008.911**

Configure the ERL and ELIN

Step 1 Choose **ERL > Conventional ERL**.
CER opens the Find and List ERLs page.

Step 2 Click **Add New ERL**.
CER opens the ERL Information window.

Step 3 In the **ERL Information** window, configure the following in the ELIN Settings section:

- Route/Translation Pattern— <RTPERL>, Route Pattern for the ERL configured in Cisco Unified CM.
  - To identify the route pattern, log into the Cisco Unified CM Administration page: **https://<Unified_CM_IP_Address_or_name>/ccmadmin**, for example: **https://10.52.211.144/ccmadmin**.
  - Choose **Call Routing > Route/Hunt > Route Pattern**,
  - Select **ends with** as the search pattern.
  - Add **911** to the search box and click **Find**. This Route Pattern should be used in CER, for example: **24085550008.911**
- ELIN—<ELINERL>, for example **4085550008**
- Onsite Alert Settings—Highlight the available IDs under Available Onsite Alert IDs and click **Add**

Step 4 Add ALI data.
For detailed information refer URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911page.html#wp1009232

Note At this stage you can assign the switch ports to the created Emergency Response Location (ERL). However it is also possible to assign a large number of ports to ERLs at one time by importing a file that contains the required information. For further details on how to assign switch ports to ERLs, please go to the following section of the CERAdministration Guide:
http://www.cisco.com/en/US/docs/voice_ip_comm/cer/7_1_1/english/administration/guide/e911conf.html#wp1050998

CHAPTER 9

Provisioning NAT/PAT Support

This chapter describes the steps required to configure the Hosted UCS platform when a Cisco NAT/PAT router or firewall connects the IP phones and the VOSS USM server. This functionality was tested in Hosted UCS Release 5.1(b), Maintenance Release 1 (MR1). This chapter includes the following sections:

Support for NAT/PAT

This section describes support for NAT/PAT through autoregistration of IP phones when VOSS USM and the DHCP server are connected by a Cisco router or firewall providing NAT/PAT services. It includes the following topics:

Support for NAT/PAT Through Autoregistration of IP Phones

In Hosted UCS deployments before Release 5.1(b), MR1, DHCP services were always managed directly by VOSS USM. USM depended on IP address information from the DHCP server to determine the location of phones, and this was a dependency for the USM AutoMove feature.

When USM manages DHCP services, Hosted UCS supports a centralized pool of DHCP servers for each customer. Two customer locations in different subnets connected to a common PAT router cannot be supported because USM associates every location with an IP address subnet. As a workaround, separate IP address pools can be created on the PAT router. However, if the DHCP server and USM server are separated by a NAT/PAT router, this scenario is not supported.

Note If two locations share the same subnet, phones cannot auto-register using the shared subnet. Configuration of shared subnets through the USM GUI is disabled in Release 5.1(b), MR1, but may still occur using bulk loaders.

Hosted UCS Release 5.1(b), MR1, now supports DHCP services that are *not* managed by USM. This allows the DHCP server to be separated from the USM server by a Cisco NAT/PAT device, such as a Cisco IOS software router, PIX firewall, or Adaptive Security Appliance (ASA). In this scenario, information required for the USM AutoMove feature is received through the syslog messages provided by the Unified CM Server.

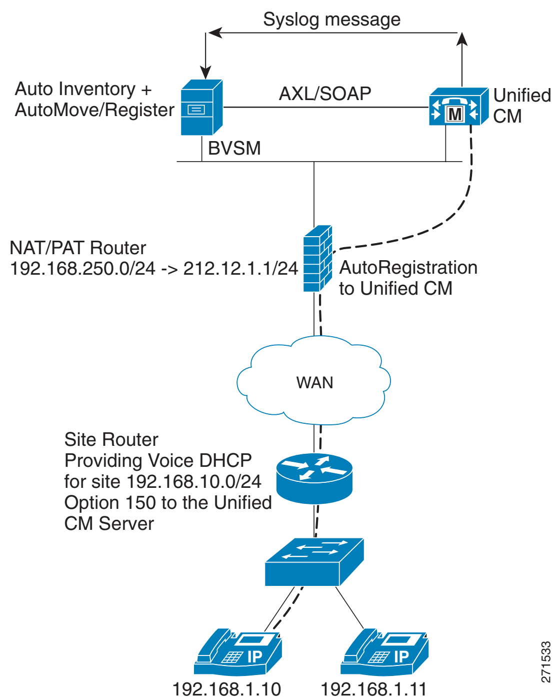
Supported Scenarios for DHCP Services

USM now supports DHCP services in the following scenarios, using auto-registration provided by the Unified CM server:

- DHCP services managed by USM, running on the USM server
- DHCP services managed by USM, running on an external server
- DHCP services *unmanaged* by USM, running on an external server
- DHCP services unmanaged by USM, running on an external server separated by a Cisco NAT/PAT device (see Figure 1).

Scenarios that are still unsupported are described in "Limitations in Support for NAT/PAT" section on page 9-3.

Figure 1 Unmanaged DHCP with Support for NAT/PAT (IP Phone Autoregistration)



How IP Phone Autoregistration Provides NAT/PAT Support

As shown in Figure 1, when the USM server receives a syslog message from Unified CM, the AutoReg service picks it up from the log and triggers the AutoCCMNewPhone transaction in USM. This transaction performs the following steps:

1. The transaction looks up the MAC address in the phone inventory and if the phone is missing, adds the phone to the inventory at the provider level.
2. If USM has not identified a location for the phone, the transaction initiates an AutoMove transaction to move the phone to the correct location in an unregistered state.
3. If the IP address received in the syslog message from Unified CM does not match the IP address in USM, the transaction updates the USM database with the new IP address.
4. If the phone is not registered in the location and the Auto-register option is selected, the transaction registers the phone.

   This completes the transaction and the phone is fully registered in USM with an allocated extension number.

USM performs all four steps when a new phone is added and Auto-register is turned on for the location. If the IP address for an existing phone is changed, only Step 3 occurs.

Limitations in Support for NAT/PAT

When the DHCP service runs on an external server and is *managed* by USM, the DHCP server and the USM server *cannot* be separated by a NAT/PAT device.

Currently, overlapping IP addresses are supported only if a separate DHCP server is used for each customer.

When USM manages the DHCP server, customer locations in different subnets connected to a common PAT router are not supported because USM associates every location with an IP address subnet. As a workaround, separate IP address pools can be created on the PAT router. However, if the DHCP server and USM server are separated by a NAT/PAT router, this scenario is not supported.

Provisioning Unified CM to Support NAT/PAT

This section describes the configuration required to provision the Unified CM server to support IP phones connected to the USM server through a Cisco NAT/PAT device. It includes the following topics:

- Auto-registration, page 9-3
- Configuring Auto-registration, page 9-4

Auto-registration

Auto-registration automatically assigns directory numbers to new devices as they connect to the IP telephony network. When auto-registration is enabled, a range of directory numbers is specified so that Cisco Unified CM can assign an unused number to each new phone that is connected to the network. As new phones connect to the network, Cisco Unified CM assigns the next available directory number in the specified range. After a directory number is assigned to an auto-registered phone, the phone is moved to a new location, and its directory number remains the same. This task is accomplished by sending the

Unified CM syslog messages to the USM server. This automatically triggers a transaction that moves the phone to the location, as explained in the "How IP Phone Autoregistration Provides NAT/PAT Support" section on page 9-3.

Configuring Auto-registration

To configure auto-registration on the Unified CM server, complete the following steps:

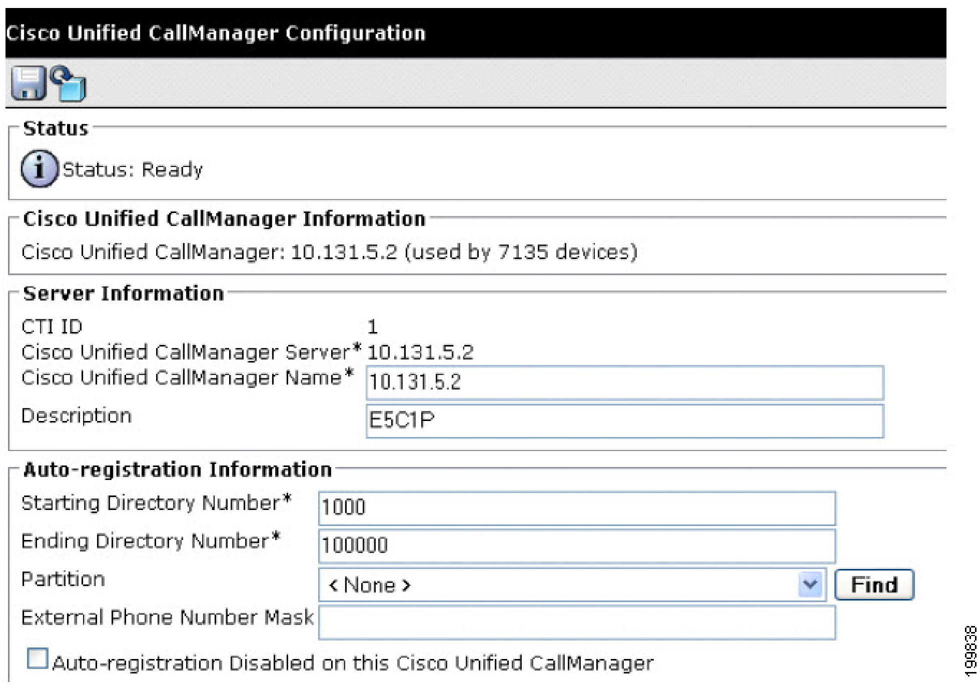
Procedure

Step 1 Connect to the Unified CM server that you need to configure.

Step 2 Choose **System** > **Cisco Unified CallManager.**

Step 3 The system displays the screen shown in Figure 9-2.

Figure 9-2 Auto-registration – Unified CM Configuration



Step 4 Make sure that **Auto-registration Disabled on this Cisco Unified CallManager** is unchecked.

Perform this step for all the Unified CM servers.

Step 5 Choose **System** > **Cisco Unified Call Manager Group**.

Step 6 Enter the group used in the Name field and check **Auto-registration Cisco Unified CallManager Group**.

Step 7 Choose **System** > **Enterprise Parameters Configuration** screen.

Step 8 Choose the correct protocol (SIP or SCCP) from the **Auto-registration Phone Control Protocol** pull-down selection list.

Note Perform this step for Unified CM 5.1 and above. Unified CM 4.X supports only the SCCP protocol.

Step 9 To direct Unified CM Syslog Messages to the USM Server, select **Cisco Unified CallManager** > **Alarm Configuration**.

Step 10 In the Remote Syslogs section, type the IP address of the USM server in the Server Name field.

Step 11 Click **Save**.

Provisioning USM to Support NAT/PAT

This section describes the configuration required for the USM server when it is connected to IP phones by a Cisco NAT/PAT device. It includes the following topics:

- Configuring USM Webmin, page 9-5
- USM Provider Configuration, page 9-8
- USM Customer Configuration, page 9-9
- USM Location Administration, page 9-9

Configuring USM Webmin

To complete the configuration required using USM Webmin, complete the following steps:

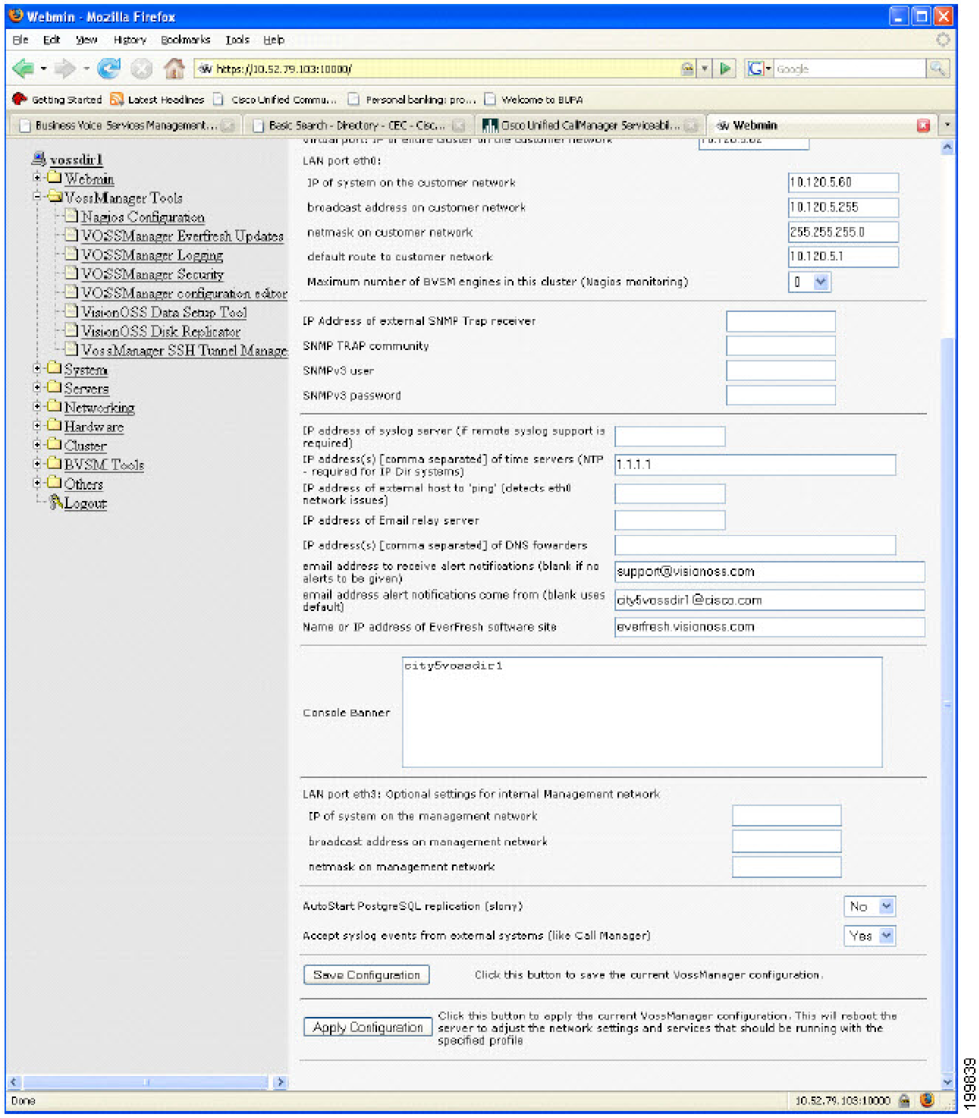
Procedure

Step 1 Access USM Webmin.

Step 2 Choose **VossManager Tools** > **VossManager configuration editor.**

The system displays the screen shown in Figure 9-3.

Figure 9-3 USM Webmin Syslog Configuration



Step 3 Choose **Yes** from the **Accept syslog events from external systems (like call Manager)** pull-down selection list.

Step 4 Choose **USM Tools** > **USM Auto Inventory and Move Phones**.

Step 5 In the Logfile Path field, type the following path:

```
/data/intdhcp/allmessages
```

Step 6 Click **Start** and **Auto-start**.

Step 7 To reboot the USM server, select **USM Tools** > **USM environment tuneup tool**.

Note After making changes to the USM server configuration, you must reboot the server to enable the changes.

Step 8 Click **Reboot**.
The USM server reboots and the new configuration is enabled.

Step 9 To verify correct syslog configuration for the USM server, establish an SSH session to the USM server using the administrator username/password.

Step 10 To display the messages received by the USM server, enter the following command:

```
cd /data/intdhcp/
tail -f allmessages
```

Step 11 To test the configuration, reset a phone on the Unified CM server, and renter the **tail -f allmessages** command.

Step 12 Verify that the syslog message generated after resetting the phone on the Unified CM server has been received by the USM server.

Configuring DHCP Services on an External Server

To configure DHCP services running on an external server, complete the following steps on the webmin of the external DHCP server:

Procedure

Step 1 Choose **Voss ManagerTools** > **VossManager Configuration**.

Step 2 Select **IP Director + Telephony DHCP (Primary)** from the **Select functional role of this machine** pull-down selection list.

Step 3 Click **Save Configuration** and **Apply Configuration** to save and apply the configuration.

Step 4 Choose **USM Tools** > **USM Auto Inventory and Move Phones.**

Step 5 In the USM URL or IP address, type the IP address or URL for the USM server.

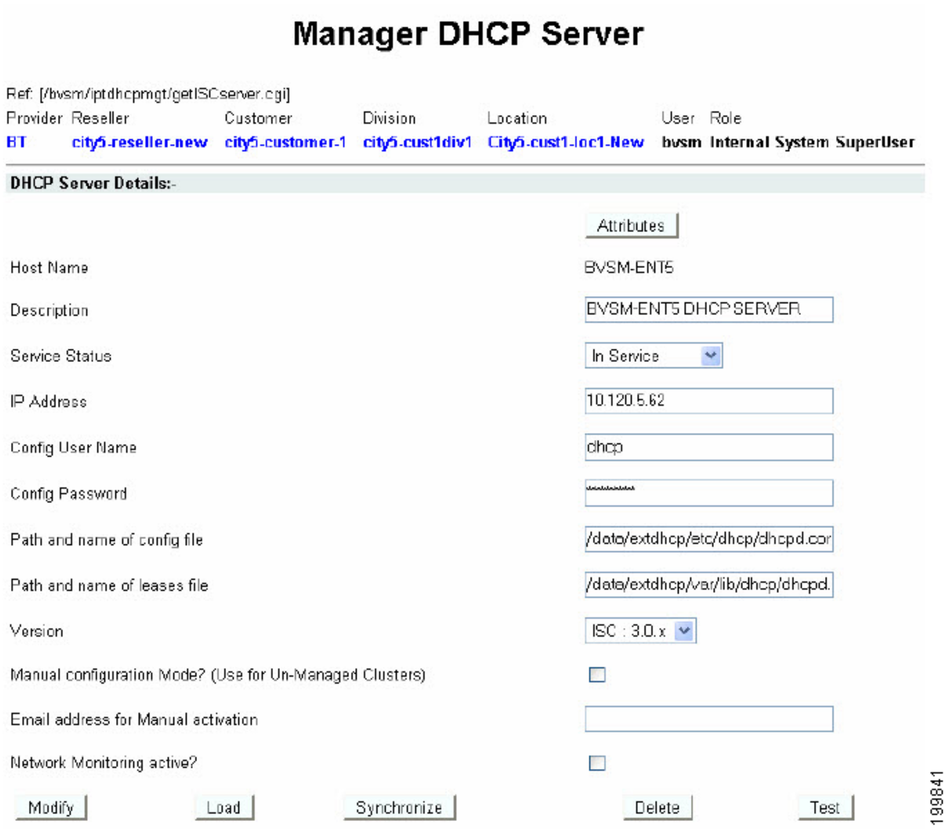
Step 6 Click **Save** and **Start** to save the settings and start the AutoMove feature.

USM DHCP Configuration

The configuration for a DHCP server managed by USM is similar whether it runs on the USM server or on an external server. However, you use the IP address of the USM server if the DHCP service is running on the USM server machine. You use the IP address of the external server if the DHCP service is running on a different machine.

Figure 9-4 illustrates the screen used in the USM GUI to configure the DHCP service.

Figure 9-4 USM DHCP Configuration



Make sure, once the DHCP server is defined on USM, the server is Loaded and Synchronized.

USM Provider Configuration

To configure the USM server to receive Auto-register requests from the Unified CM server, complete the following steps:

Procedure

Step 1 Choose **Setup Tools** > **Global Settings** > **AutoCCMNewPhoneProvider**.

Step 2 Choose the provider to which the Auto-register daemon reports.

Step 3 Choose **Setup Tools** > **Global Settings** > **PAT-IP-Reuse.**

Step 4 Enable the **Current Setting** checkbox.

This setting is used when phones register with the same IP address (PAT).

Step 5 Choose **Provider** > **Select a provider** > **Preferences** > **ProviderAllowAutoPhoneInventory.**

Step 6 Enable the **Current Setting** checkbox.
This causes USM to automatically add phones discovered through Auto-registration to the Phone Inventory.

USM Customer Configuration

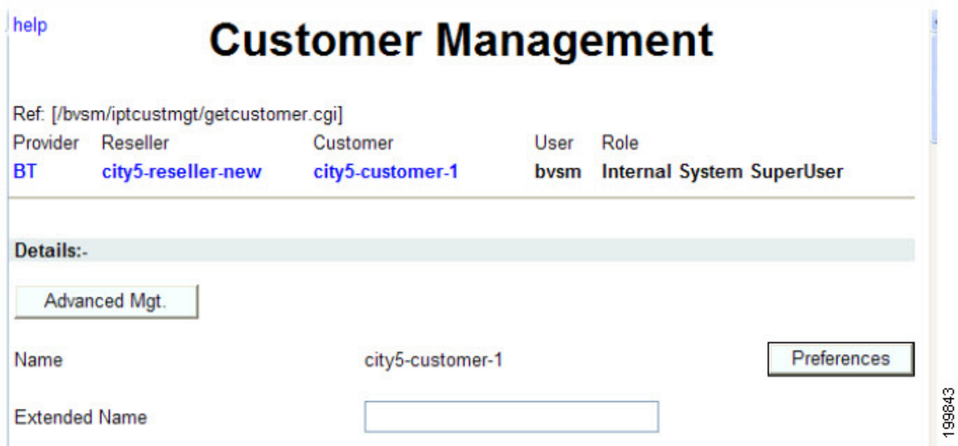
To complete the Customer configuration required on the USM server, complete the following steps:

Procedure

Step 1 Choose the customer for which you want to enable the AutoMoveCustomer option.

The system displays the screen shown in Figure 9-5.

Figure 9-5 Customer Management



Step 2 Click **Preferences.**

Step 3 Click **AutoMoveCustomer**.

Step 4 Enable the **Current Setting** checkbox.

Step 5 On the Preferences and Settings screen, click **XML-PhoneAutoRegistration**.

Step 6 Enable the **Current Setting** checkbox.

Step 7 On the Preferences and Settings screen, click **ShowCorporateDir**.

Step 8 Enable the **Current Setting** checkbox.

USM Location Administration

Step 1 Choose the Location for which you need to enable the AutoMove feature.

Step 2 Click **Preferences** and select the **AutoFeatureLocation** option from the Preferences and Settings: Location screen.

Step 3 Choose the appropriate feature group, such as **COS1International24Hour**.

Step 4 From the Preferences and Settings: Location screen, select the **AutoMoveLocation** option.

Step 5 Enable the **Current Setting** checkbox.

Step 6 From the Preferences and Settings: Location screen, select the **AutoRegister** option.

Step 7 Enable the **Current Setting** checkbox.

Step 8 From the Preferences and Settings: Location screen, select the **AutoRegisterLowestLocation** option.

Step 9 In the Current Setting field, type the starting phone extension number used on the Unified CM server.

Step 10 Save the configuration changes and reboot the USM server to enable the new configuration.

CHAPTER 10

Provisioning Other Hosted Unified Communications Services Features

This chapter describes how to use VisionOSS Unified Services Manager (USM) application to provision the components of the Cisco Hosted Unified Communications Services (UCS), Release 7.1(a) platform.

It details how to use the application to manage the various Hosted UCS features of a Cisco Multi-tenant Hosted Unified Communications Services (UCS) 7.1(a) deployment.

This chapter includes the following sections:

Provider Specific Features

Cisco Hosted Unified Communications Services, Release 7.1(a) introduces support for provider specific features.

This section describes the required steps to provision a provider or per-country provider specific features in a Cisco Hosted UCS 7.1(a) environment.

This section contains:

- Forced Central PSTN Breakout, page 10-2
- Forced OffNet, page 10-3
- Forced Authorisation Codes (FAC), page 10-4

Forced Central PSTN Breakout

The Cisco Hosted UCS 5.1(b) platform extends support to the Forced Central PSTN Breakout functionality.

You can configure the Cisco PGW using USM to analyze the outgoing PSTN calls and to “force” the use of the central gateways for some PSTN destinations. Additionally, the Administrator can provision a subset of these numbers to be “allowed” to use the local gateway.

The following section explains how to configure the Forced Central PSTN Breakout in two ways:

- Forced To Use, page 10-2
- Allowed To Use, page 10-3

Forced To Use

To provision a range of numbers to be “Forced” to use Central Gateways, perform the following steps:

Procedure

Step 1 Go to **Provider Administration > Providers**.

Step 2 Select the provider you want to configure, from the Search Results area.

Step 3 Click **Advanced Mgt.**.

Step 4 Click **International Gateway Usage**.

Step 5 Select the Cisco PGW that you want to configure, from the Search Results area.

Step 6 Click **Add**.

Step 7 Enter the following:

- Country: <country>, for example, `United States`
- National Code: Although it says National Code, you can enter any part of a E.164 number (even the full E.164 number if you want to “Force” only one number to go out through the Central PSTN Breakout), for example `212211`

Step 8 Select Force Central.

Note Country and Gateway Usage are mandatory fields.

Step 9 Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

Allowed To Use

To provision a range of numbers to be "Allowed" to use Local Gateways, perform the following steps:

Procedure

Step 1 Go to **Provider Administration > Providers.**

Step 2 Select the provider you want to configure, from the Search Results area.

Step 3 Click **Advanced Mgt.**.

Step 4 Click **International Gateway Usage**.

Step 5 Select the Cisco PGW that you want to configure, from the Search Results area.

Step 6 Click **Add**.

Step 7 Enter the following:

- Country: <country>, for example, `United States`
- National Code: Although it says National Code, you can enter any part of a E.164 number (even the full E.164 number if you want to "Force" only one number to go out through the Central PSTN Breakout), for example `2122112`

Tip The example numbers mentioned will force all numbers in the ranges from 212-211-0000 to 212-211-1999 and from 212-211-3000 to 212-211-9999 to use the Central PSTN Breakout.

Step 8 Select Allow Local.

Step 9 Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

Repeat this procedure for all providers.

Forced OffNet

Cisco Hosted UCS 7.1(a) extends support to the Forced OffNet facility.

It allows you to configure the Cisco PGW using USM to analyze outgoing PSTN calls and to "Force" all OffNet calls to go out of the Hosted UCS environment, even if the destination is a user in the Hosted UCS environment.

The following section explains how to configure the Forced OffNet option.

To provision a range of numbers to be “Forced” out of the Hosted UCS environment, perform the following steps:

Procedure

Step 1 Go to **Provider Administration > Countries**.

Step 2 Select the Country you want to configure, from the Search Results area.

Caution Ensure to add a reseller for the correct provider. It displays the name of the provider.

Step 3 Click **Force OffNet**.

Step 4 In the Add Prefix area, enter the following:

- Prefix <Prefix>, enter the E.164 number prefix which will define the range of E.164 numbers to be “Forced” Offnet, for example: `441630212`
- Country Code

Tip The example prefix mentioned will force all numbers in the range from 441630212000 to 441630212999 out of the Hosted UCS environment.

Step 5 Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

Repeat this procedure for all providers.

If you were to upgrade to Cisco Hosted UCS 7.1(a), the Administrator deletes existing “Forced” OffNet configurations.

This occurs when you provision “Forced” OffNet in Cisco Hosted UCS 5.1(b) by replacing the PGW transaction (used for the “Forced” Central PSTN Breakout feature in the PGW model) with the PGW transaction required for the “Forced” OffNet feature, and then utilize the USM interface to provision “Forced” Central PSTN Breakout.

After upgrading to Cisco Hosted UCS 7.1(a), the Administrator must re-provision the previously configured numbers using the provisioning procedure as described in Forced Central PSTN Breakout.

Forced Authorisation Codes (FAC)

Forced Authorization Codes (FACs) allow administrators 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. Each FAC has three items of data associated with it, and is associated to a route pattern. Following sections describes how to provision FAC on HUCS 7.1a deployment.

- FAC Static Configuration, page 10-5
- Add Forced Authorization Codes, page 10-5
- Move FAC to a Location, page 10-5

FAC Static Configuration

FAC on CUCM is associated with Route Patterns. Hence, route patterns which require FAC need to be updated on CUCM.

Step 1 Find the Route Patten on CUCM which require FAC. If you want outgoing central break-out PSTN calls on a location to use FACs, search for the PSTN route pattern for that location in CUCM, for example, search for **9.01[2-9][02-9]XXXXXXX** route pattern which require FAC. You can use CUCM Digit Analyzer, in case you are not sure of which route pattern is chosen for the dialed number.

Step 2 Check **Require Forced Authorization Code** check box

Step 3 Set Authorization Level, default **0.**

Note Authorization Level for a route pattern should be lesser than the FAC code authorization level for call completion using FAC. Otherwise, call routing to dialed number through that Route Pattern would fail.

Add Forced Authorization Codes

To add provision FACs on CUCM via USM, follow the steps below:

Step 1 Navigate to **Resources > Authorisation Codes** at provider level.

Step 2 Click **Add Range.**

Step 3 Under Details section, enter the following:

- Range Start—<FACRangeStart>; for example, **1234**
- Name—<FACname>; for example, **FACTOPSTN**
- Level—<AuthorisationLevel>; for example, **2**
- Range Size—<CodeRangeSize>; for example, **1**

Step 4 Click **Add Range**.

Note Authorization Level for a route pattern should be lesser than the FAC code authorization level for call completion using FAC. Otherwise, call routing to dialed number through that Route Pattern would fail.

Move FAC to a Location

After adding a FAC, it should be moved to location to which FAC is required.

Procedure:

Step 1 Navigate to **Resources > Authorisation Codes** at provider level.

Step 2 Click **Assign** on the FAC which you want to move to a location, under the column Assign/Release.

Step 3 Enter the Range Size; for example, **1**

Step 4 Select the Location.

Step 5 Click **Assign Range.**

Customer Specific Features

This section describes the steps required to configure customer specific features in a Cisco Hosted UCS 7.1(a) environment.

Note The steps mentioned in this section are optional. If the HUCS7.1a deployment requires the customer specific features mentioned in this section, then following steps are to be performed based on features requirement

Cisco Hosted UCS 7.1(a) supports the Block OffNet To OffNet Transfer (BO2OT) customer specific feature.

It is possible to configure a customer using USM, to block a user in a Hosted UCS IP location from transferring an incoming call from the PSTN back to the PSTN.

This section contains the following:

- Enable BO2OT on Unified CM, page 10-6
- Configure BO2OT for Customers, page 10-6

Enable BO2OT on Unified CM

To provision Unified CM to enable the Block OffNet To OffNet Transfer (BO2OT) parameter, perform the following steps:

Procedure

Step 1 Login to CUCM cluster.

Step 2 Navigate to System > Service Parameters.

Step 3 Select the CUCM server.

Step 4 Select the Cisco CallManager service.

Step 5 Under Clusterwide Parameters (Feature - General), set Block OffNet To OffNet Transfer to **True.**

Step 6 Click **Save.**

Configure BO2OT for Customers

To provision a specific customer to Block OffNet To OffNet Transfers, perform the following steps:

Procedure

Step 1 Choose **General Administration > Customers**.

Step 2 Select the customer you want to configure, from the Search Results area.

> **Caution** Ensure that you are configuring customers for the correct reseller.

Step 3 Navigate to Customer for which BO2OT is required.

Step 4 Click **Advanced Mgt.**

Step 5 Click **Advanced Telephony Settings**.

Step 6 Click **Enable** next to Block Offnet to Offnet Transfer**.**

Location Specific Features

This section describes the steps required to configure location specific features in a Cisco Hosted UCS 7.1(a) environment.

> **Note** The steps mentioned in this section are optional. If the HUCS 7.1a deployment requires the location specific features mentioned in this section, then following steps are to be performed based on features requirement.

The following section lays emphasis to the support for overlay area codes that was initially introduced in the Cisco Hosted UCS 5.1(b).

Two principle methods are used to provide numbering relief to NPAs nearing exhaustion:

- NPA Overlay, page 10-7
- NPA Geographic Split, page 10-8

NPA Overlay

An overlay is an alternative way of adding an area. As the name suggests, the new area code "overlays" the pre-existing area code, most often serving the identical geographic area. Numbers from this new NPA are assigned for new growth to all service providers and customers.

In the United States, according to the FCC ruling in the Second Report and Order (R&O) in CC Docket 96-98, the implementation of an NPA overlay for code relief will require a 10-digit dialing within and between NPAs for local calls to ensure dialing parity among all service providers.

The benefit of an NPA overlay is that customers retain their existing area codes. Only new lines get the new area code.

An overlay requires all customers, including those with telephone numbers in the pre-existing area code, to dial area codes for local calls.

NPA Geographic Split

Most area codes are added by way of a geographic split. The geographic area covered by an existing area code is split in two (or three). One of the sections retains the existing area code (usually the area with the highest customer density to minimize number changes), while others receive new area codes.

The benefit of a geographic split is that an area code remains defined as a geographic area which gives the customers a fairly good idea about the location of the people they are calling.

The down-side of a geographic split is that many customers must cope with the inconvenience of changing their area code.

This section describes the required procedure to define an Overlay Area Code in US Locations with a 10-digit local dialing support. Once the code is configured, a user in these locations can make local calls to a phone in the Overlay Area Code by dialing the "External Prefix" followed by NPA-NXX-XXXX (where NPA is the configured Overlay Area Code).

Add Overlay Area Codes

Overlay Area Codes are defined in USM as Adjacent Area Codes.

Note Overlay Area Code in Hosted UCS7.1a is supported only for location with central PSTN breakout. Location with local PSTN breakout does not support this feature

To add an Overlay Area Code, perform the following steps:

Procedure

Step 1 Choose **General Administration > Locations**.

Step 2 Select a location for which you want to assign an Overlay Area Code.

Caution Ensure that you are adding the Overlay Area Code for the correct location.

Step 3 Click **Advanced Mgt.**.

Step 4 Click **Adjacent Area Codes**.

Step 5 Click **Add**.

Step 6 For Enter Adjacent Area Code, enter <OverlayAreaCode>, for example `646`

Step 7 Click **Add**.

Repeat this procedure for all required Overlay Area Codes and for all locations.

Phone Specific Features

This section helps you configure phone specific features in a Cisco Hosted UCS 7.1(a) environment.

Support for XML Phone Application was tested for the first time on Hosted UCS 7.1 (a).

It is possible to configure the Unified CM IP phones to access different XML applications. The Services button on the Cisco Unified CM IP phone helps you select the Phone Services option to access these XML applications.

This section describes three functions you can perform for the XML application:

- Create Service Type for the XML Phone Service, page 10-9
- Add XML Phone Service to a Feature Group, page 10-9
- Personalize phone with XML Application, page 10-10

Create Service Type for the XML Phone Service

To configure a new phone service, perform the following steps:

Procedure

Step 1 Go to **Setup Tools > Service Types**.

Step 2 Click **Add**.

Step 3 Provide a Service Name. For example, `Calendar`

Step 4 Provide a description. For example, `Calendar Phone Service`

Step 5 Provide a tag. For example, `Calendar`

Step 6 Select the Service Category. For example, `phoneapplication`

Step 7 Provide the URL of the service. For example,
`http://10.100.92.33/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME#`

Step 8 Click **Add** to create the Phone Service.

Add XML Phone Service to a Feature Group

To use the already created phone service, you need to add the service to a customer feature group.

To do this, perform the following steps:

Procedure

Step 1 Go to **General Administration > Feature Groups**.

If you are not at customer level, you must select the customer of the feature group you want to create or modify.

Step 2 Select the feature group where you want to incorporate the phone service or create a new feature group.

Step 3 Select the phone service tag that you previously created. For example, `Calendar`

Step 4 Click **Add**.

Personalize phone with XML Application

You can personalize a phone application, which is not available in the feature groups, to other phones and user mobility profiles. You can do this when you do not want to make available a phone service for all the phones using the same feature group, but need to only add the service to a specific phone of a location.

To do this, perform the following steps:

Procedure

Step 1 Go to **General Administration > Locations**.

Step 2 Select the location where the phones you want to personalize are located.

Step 3 Click **Preferences**.

Step 4 Click **PersonalizePhoneApplications** from the list.

Step 5 Check the checkbox to enable the setting and click **Modify**.

Once you enable this preference, you can personalize any phone in that location.

Step 6 Go to **Location Administration > Phone Management**.

Step 7 Click the MAC address of the phone you want to personalize.

Step 8 Scroll down to Phone Applications area and click **Personalize**.

Step 9 Click **Subscribe**.

Step 10 From the drop down menu, select the Phone service that you created and click **Submit**.

CHAPTER 11

Provisioning Analog Gateway

This chapter describes the steps required to provision an analog VG224 gateway for a customer location in Hosted UCS Release 7.1(a).

Define and Configure VG224 Device

USM administrator defines an IOS Device (Type, Interfaces). This information is later used to add and configure the VG224 Gateways. Following sections describe how VG224 Device components are defined:

- Add VG224 Device Type, page 11-1
- Add VG224 Gateway, page 11-2
- Configure Gateway Hardware, page 11-3
- Configure Ports, page 11-3
- Allocate Port to Location, page 11-4
- Register Analog Port, page 11-4

Ensure that you are Adding IOS Device Components to the correct Provider. To get to the Provider level, do the following:

Step 1 Go to **Provider Administration > Providers**.

Step 2 Select a Provider.

Add VG224 Device Type

To add an IOS Device Type:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click **Add.**

Step 3 Click **Add** corresonding to **IPPBX Connect MGCP VG2xx Analog Gateway.**

Note VG224 analog gateway can be provisioned with CUCM using MGCP, SCCP and SIP protocols. Select the appropriate option to add VG224 device based on the deployment and protocol.

Step 4 Under Device Details, enter the following :

- Host Name—Unique <Host name of the IOS Device>; for example, **e2vg224**
- Description—<IOSDeviceTypeDesc; for example, **City2 VG224 analog gateway**
- Country—Select <Country>; for example, **United Kingdom**
- Owner—Select <Provider>; for example, **UKprovider**
- Check **Single Location Only** check box.

  Note When you enable Single Location Only, the IOS device can be used in the selected location only.

- Select Location—Select the location from the drop down list; for example, **Reseller_A: Customer_A: Division A: 1402Clu2Loc1**

Step 5 Under Connectivity Details, enter the following:

- IP Address—<EthInterface IP Address>; for example, **10.190.2.42**
- IP Address (alternate)—<Alternate IP Address>; for example **10.191.2.42**
- IP Domain—<Domain name>; for example **e2vg224**
- Config Password—Enter <IOS device config password>; for example, **cisco**
- Enable Password—Enter <IOS device enable password>; for example, **cisco**

Step 6 Click **Finish.**

Add VG224 Gateway

To add a Media Gateway, do the following:

Step 1 Choose **Network > IOS Devices.**

Step 2 Click the IOS Device, for example **e2vg224.**

Step 3 Under Device Roles, click **Add** on Gateway

Step 4 Under Gateway Details, ensure the following:

- Name—<GW hostname>; for example, **e2vg224**
- Description—<GW description>; for example, **City2 VG224 analogue gateway**
- Select Protocol, for example **MGCP**

Step 5 Click **Next.**

Step 6 Select Device, <IPPBX: e2c1p, version: 7.1.x>

Step 7 Click **Next**.

Step 8 Under Gateway Functions, select analog for location.

Step 9 Click **Add.**

Repeat this for all IOS Device Network Modules.

Configure Gateway Hardware

To configure gateway hardware, do the following:

Step 1 Go to **Network > IOS Devices**.

Step 2 Click the IOS Device; for example, **e2vg224.**

Step 3 Click the Gateway under Gateway Details; for example, **e2vg224.**

Step 4 Click the **Gateway Hardware Configuration**, under Interface Details.

Step 5 Under Gateway Information, enter the following:

- Gateway Chassis—Select the gateway chassis; for example **VG224.**
- Click **Next**
- Module Slot—Select Module type **ANALOG**
- Click Next
- Under Module Slot, select the Voice Interface Card; For example, **24 FXS**
- Gateway Voice Interface—<GatewayInterface>; for example, **FastEthernet0/0**

Step 6 Click **Save.**

USM retrieves the module analog port details and updates the gateway hardware configuration page with port details.

Configure Ports

To add and configure gateway ports, do the following:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click the IOS Device; for example, **e2vg224.**

Step 3 Click the Gateway under Gateway Details; for example, **e2vg224.**

Step 4 Click the **Gateway Hardware Configuration,** under Interface Details.

Step 5 Click the port you want to configure; for example, **0 FXS**.

Step 6 Under Device Information, ensure the following:

- Phone Button Template—<PhoneButtonTemplate>, select **Standard Analog.**
- Under Location Specific Settings, enter the following:
- Signal—<SingnalType>; for example **select Ground Start**

Step 7 Click **Add**

Allocate Port to Location

To allocate analog port to a location, follow the steps below:

Step 1 Go to **Network > IOS Devices.**

Step 2 Click the IOS Device; for example **e2vg224.**

Step 3 Click the Gateway under Gateway Details; for example **e2vg224.**

Step 4 Under Analog Interfaces, Click **Port Allocation.**

Step 5 Under Unallocated Ports, ensure that the location selected is proper and tick the port

Step 6 Click **Allocate.**

Register Analog Port

In Hosted UCS 7.1(a), the analog gateway port registration is done at location level. To register an analog FXS port:

Step 1 Navigate to the location where the analog gateway is provisioned, for example **1402Clu2Loc1.**

Step 2 Choose **Location Administration > Analogue Line Mgt**.

Step 3 Click the Analog gateway hyperlink; for example, **e2vg224**

Step 4 Click **Register** for the analog port you want to register with CUCM.

Step 5 Select the feature group; for example, **COS1International24Hour.**

Step 6 Click **Next**

Step 7 Under Line Number 1, select the number; for example, **DDI 014022118001**

Step 8 Select the Line Class of Service; for example, **COS1International24Hour**

Step 9 Click **Register.**

Note The automatic MGCP provisioning feature will automate the global MGCP configuration with the use of the following two commands. If MGCP autocomple commands are disabled on the "IOS Device 12.x - Model MGCP" and you need MGCP automatic provisioning, then add the following commands on MGCP analog gateway configuration.

- e2vg224# ccm-manager config server <TFTP1IPADDR>
- e2vg224# ccm-manager config

TFTP1IPADDR is the IP address of the CUCM server where TFTP Service is running.

CHAPTER 12

Provisioning Linked Locations

New Linked Locations functionality on Hosted UCS 7.1A allows a single site code to be shared within a group of locations called linked locations. This allows 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 of linked location groups, 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 are as follows:

- Site Code
- Extension Length
- Hardware Group
- PBX Template
- Global site partition

All other settings/resources for a child location are independent of the parent (e.g. published number, emergency number, voicemail, gateways, etc). In the case of Hosted UCS, the bulk of the dial plan is independent between the parent and child for the CCM and PGW models.

To define and configure Linked Locations (Shared SLC), do the following:

- Configure a Linked Location Parent, page 12-1
- Add a Linked Location Child, page 12-2
- Manage E.164 Inventory, page 12-3
- Hunt Group/Number Groups for Linked Locations, page 12-3

Configure a Linked Location Parent

A Linked location parent can be configured via USM either by converting an exiting Standard location to a Linked location under a Customer or by adding a new linked location parent. Follow either of the sections below to configure a linked location parent

- Convert a Standard Location to Linked Location Parent
- Add a new Linked Location Parent

> **Note** Follow one of the following sections based on your location configurations.

Convert a Standard Location to Linked Location Parent

Step 1 Choose **General Administration > Locations**

Step 2 Click the Standard Location which you want to convert to Linked Location Parent.

Step 3 Check the **Linked Location Parent** check box

Step 4 Click **Modify**.

Add a Linked Location Parent

To add a new linked location parent under a Customer, follow the steps below:

Step 1 Choose **General Administration > Locations.**

Step 2 Click **Add**, to add a new location.

Step 3 Under Location details, enter the following:

- Location Name—<LocName>; for example, **Cus1Div1LLParent**
- Address1—<Address>
- City—<CityName>; for example, **Reading**
- Country—Select the <Country>; for example, **United Kingdom**
- Post/Zip Code—<PostCode>; for example, **RGB 6G2**
- Contact Name—<ContactPerson>; for example, **Yuvaraj**
- Select the Location Type to be **Linked Location Parent**

Step 4 Click **Next.**

Step 5 Under Hardware Group , select the hardware group, for example, **pgw2-e2c2-hwgrp.**

Step 6 Under Site Code and area code, enter the appropriate values.

Step 7 Under Subnets, Select the IP subnet to that location.

Step 8 Click **Next** .

Step 9 Under Phone Types and Number, enter the appropriate values

Step 10 Click **Add.**

Add a Linked Location Child

To add a Linked Location Child, under the same Customer as Parent

Step 1 Choose **General Administration > Locations**

Step 2 Click **Add.**

Step 3 Under Location details, enter the following:

- Location Name—<LocName>; for example **Cus1Div2LLChild1**
- Address1—<Address>
- City—<CityName>; for example, **Reading**
- Country—Select the <Country>; for example, **United Kingdom**
- Post/Zip Code—<PostCode>; for example, **RGB 6G2**
- Contact Name—<ContactPerson>; for example, **Yuvaraj**
- Select the Location Type to be **Linked Location Child**
- Select the Linked Location Parent from drop-down menu; for example, **UKDivision1: Cus1Div1LLParent (Site Code : 111)**

Step 4 Click **Next.**

Step 5 Under Dial Plan , select Dial this to get outside line; for example, **9**

Step 6 Select Default Area Code; for example, **1402**

Step 7 Under Subnets, Select the IP subnet to that location.

Step 8 Click **Next**

Step 9 Under Phone Types and Number, enter the appropriate values

Step 10 Click **Add**.

Manage E.164 Inventory

Managing E.164 inventory for linked locations is same as standard location. To create E.164 numbers, associate E.164 numbers with internal extensions for linked locations, please refer Creating an E.164 Inventory, page 4-2.

Hunt Group/Number Groups for Linked Locations

Note The steps listed in this section are optional and required only if you want to configure hunt group or number group for linked locations.

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, do the following:

Step 1 Choose **Location Administration > Number Groups.**

Step 2 Select the linked location in which the number group needs to be added

Step 3 Select **Add**.

Step 4 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.

Step 5 Select the appropriate line numbers and enter other details

Step 6 Click **Add.**

CHAPTER 13

Provisioning Single Number Reach

Cisco Unified Mobility application known as Mobile Connect, commonly called Single Number Reach (SNR), provides Cisco Unified Communications users with the ability to be reached via a single enterprise phone number that rings on both their IP desk phone and their cellular phone (Remote Destination), simultaneously. Mobile Connect users can pick up an incoming call on either their desk or cellular phones and at any point and can move the in-progress call from one of these phones to the other without interruption.

Hosted UCS 7.1a supports provisioning Single number reach. It allows a user to create a remote destination number and associate one or more internal extensions to it. If this feature is enabled on the Call Manager the call will be forwarded to the remote destination number as well, hence the concept Mobile Connect / Single Number Reach.

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 will appear for a user if it is in their feature group, however they will receive an error message if the location is not enabled for SNR ("This location does not support single number reach").

This chapter has the following sections:

SNR/Mobile Connect Static Configuration

This section details the manual (static) configurations steps required to be performed for Hosted UCS 7.1a SNR feature support. The following topics are covered in this section:

- Update CUCM Service Parameter for Mobility
- Modify and Import Softkey Template

Update CUCM Service Parameter for Mobility

Cluster wide service parameters for System - Mobility needs to be set for Hosted UCS 7.1a SNR feature, when the remote destination provisioned is a remote PSTN phone via central or local PSTN breakout.

Step 1 On each Cisco Unified CM cluster, go to **System > Service Parameters > Clusterwide Parameters (System - Mobility)**.

Step 2 Set Matching Caller ID with Remote Destination as **Partial Match.**

Step 3 Set Number of Digits for Caller ID Partial Match as **14.**

Note If the mobile enterprise features hold and resume are required to be supported for mobiliy user, then "Mobile Enterprise Feature Access" service parameter needs to be set to true on CUCM clusters

Modify and Import Softkey Template

Softkey template configuration allows the administrator to manage softkeys that the Cisco Unified IP Phones support. To hand-off SNR calls from SNR desk phone to the requied remote destination desk phone, the Mobility softkey should be configured on the Softkey template.

To add Mobility Softkey on Unified CM clusters, edit the softkey template Softkey_Advanced on the relevant CUCM cluster with Mobility key and import the softkey template into USM. For further details refer, Importing Softkey and Phone Button Templates, page 3-11

Enable SNR functionality for the user

To enable SNR functionality for the end user, the SNR needs to be enabled in the feature group that the user uses.

Procedure:

Step 1 Choose **General Administration > Feature Groups.**

Step 2 Select the Customer; for example, **Customer_D.**

Step 3 Select the Feature Group; for example, **COS1International24Hour**.

Step 4 Check **Single Number Reach / Mobile Connect capabilities** check box.

Step 5 Click **Modify.**

Enable SNR functionality for a Location

SNR needs to be enabled for a location. This can be done while adding a location or when modifying a location to enable SNR for the location. To modify a location to support SNR,

Step 1 Choose **General Administration > Locations**.

Step 2 Under Location Details, check the **Single Number Reach Support** check box.

Step 3 Click **Modify.**

Note Ensure that the location has PSTN published number configured. The mobility call extended to remote destination uses the PSTN published number of location having calling party number for the SNR call.

Add SNR Remote Destination

SNR is at a user level. USM provisioning for SNR Mobile Connect is limited to user with roaming profile/extension mobility. A roaming profile must be associated with SNR user for adding a remote destination for an extension. Please note that the user may create a Remote Destination without associating any extensions to it. This section lists the provisioning steps for adding a remote destination for an extension.

- Associate Roaming Profile for the SNR user
- Add a Remote Destination for the SNR user)

Associate Roaming Profile for the SNR user

If the SNR location user is not associated with any roaming profile (Mobility), then perform the steps mentioned in the Section Adding User Extension Mobility, chapter 4.

Add Remote Destination for the SNR user

To add a Remote Destination for an SNR user, do the following:

Step 1 Navigate to **Location Administration > Users** via hierarchy to select the user.

Step 2 Click the location user to which SNR remote destination is to be added

Step 3 On the User Management Screen, click **Single Number Reach**.

Step 4 Enter the name; for example , **Remote1.**

Step 5 Enter the number; for example, **901628100060.**

Note The SNR Name and Number are unique per Call Manager Cluster.

Step 6 Check **Mobile Phone** check box.

Note Selecting the Mobile Phone check box, will give a user the ability to hand-off any active desk phone call to the desired Remote Destination, by pressing the Mobility softkey. Once the Remote Destination answers, the desk phone will release the call.

Step 7 Check **Enable Mobile Connect** check box.

Note Selecting the Enable Mobile Connect check-box, will ring both the desk phone, as well as the Remote Destination, for incoming calls.

Step 8 Under Available extensions to user, Select the extensionss) to which remote destination is required

Note USM provisioning for SNR Mobile Phone feature (hand-off the call to remote destination by pressing "Mobility" softkey) is limited to extension mobility user who has logged to a phone. Repeat this for all remote destinations to be added for the SNR user.

APPENDIX A

Hosted Unified Communications Services Location Administration

Revised: 08/12/2010, OL-23270-01

This document describes the options available to Location-level administrators within the Hosted UCS Release 7.1(a). The options available to the Location administrator depend on the specific Hosted UCS implementation. If you have questions about the availability of a specific option, contact the customer administrator for the Hosted UCS system. The following sections introduce the Hosted UCS interface and describe the options available to the Location administrator on the General Tools menu and the Location administration menu:

User Interface Guidelines

Note the following conventions used in these menus and associated administration pages:

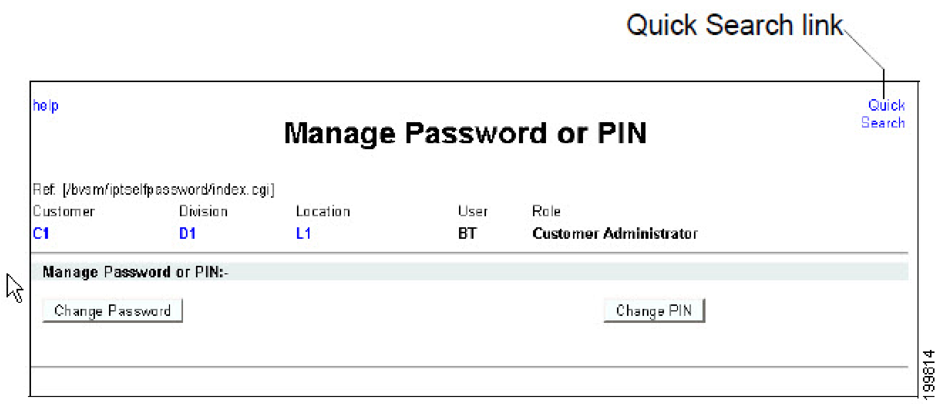
- Links to other pages are bright blue.
- Required fields are indicated by a red asterisk (*).
- Error messages are displayed in red type.
- Most changes provide a transaction record that indicates if the transaction is successful and that may provide an explanation if it is not.
- You can use the browser Back button to return to a previously viewed page, or you can click on any option in the navigation menu to go directly to a specific option.

- Changes to a page are not saved until you click the **Add**, **Submit**, or **Modify** button, which is required to complete the transaction (Add, Submit, or Modify).

Quick Search

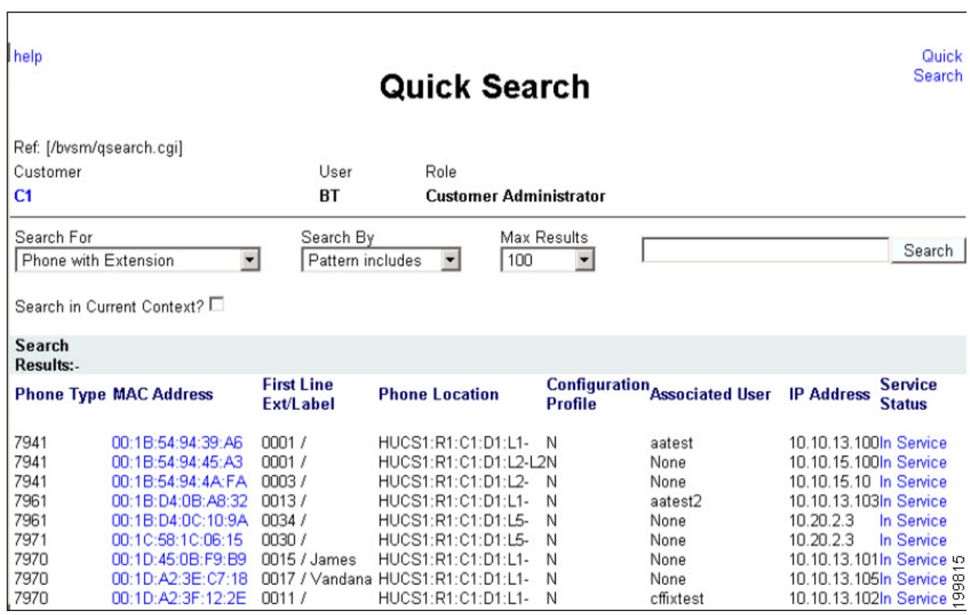
As shown in Figure A-1, each page of the USM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries to which you have access are determined by the access privileges associated with the user account that you used to log into the system.

Figure A-1 Quick Search Link



When you click the Quick Search link, the system displays the page shown in Figure A-2

Figure A-2 Quick Search Page



This page displays a list of the entries in the Hosted UCS database to which you have access.Select the options described in Table A-1 from the **Search For** pull-down selection list to identify the type of entries for which you want to search.

Click on a blue link on this page to open the management page for the selected entry. To refine your search, select one of the following options from the **Search By** pull-down selection list.

- 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.

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.

Table A-1 Search Types

Search Type	Description
Location Searches	
Location	Find a location by name within the division or customer level.
Location with Site Code	Find a specific location by entering the site code.
Location of User	Find a location by entering a user account name.
Location of Phone	Find a location by entering the Mac address of a phone.
Extension Search	
Extension	Find an extension by its numeric identifier.
Extension associated with DDI	Find an extension by entering the external line to which it is registered.
Extension used by User	Find an extension by entering the associated user account.
Extension used by Phone	Find an extension provisioned on a phone by entering the MAC address of the phone.
Mac Search	
Phone with Mac	Find a phone by entering the MAC address.
Phone with Extension	Find a phone by entering the associated extension.
Phone with DDI	Find a phone by entering the external line to which the phone is registered.
Phone with User	Find a phone by entering the associated user account name.
User Search	
Username	Find a user account by entering the user account name.
Surname	Find a user account by entering the last name associated with the user account.
Firstname	Find a user account by entering the first name associated with the user account.
User with Extension	Find a user account by entering the extension associated with the user account.

Phone Management

External (or DDI) numbers are unique E.164 numbers that are not necessarily allocated to every business phone. A call from another company can only be placed to an external (DDI) number. You cannot call an internal number from outside the company. Internal numbers are allocated to every phone. They allow internal calls to be made between staff within a company, both intra-location and inter-location. External numbers must be associated to an internal number before it can be registered with a phone, because every phone must have an internal number.

The following summarizes the process of managing numbers in the Hosted UCS system:

1. Add a phone to the Hosted UCS system.

This is normally accomplished through bulk loading the Mac address, phone type, and associated button template. However, phones can also be added at the Provider Administration level.

2. Move a phone to the location.

This step is performed from the Customer Administration level by moving the phone to a specific location. This associates the phone with the subnet where it gets its IP address assigned. After completing this step, in the USM interface, this phone will appear in an “Unregistered” state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

3. Register a phone (once registered, you can make and receive calls.

This step is performed at the Location Administration level by selecting the phone from a list of unregistered phones in the USM database. On the Phone Registration page for the selected phone, you select the feature group and allocate the DDI line number. This phone then appears in the Registered state in USM.

4. Associate a phone to a user account (once associated, the user account will be listed in the corporate directory).

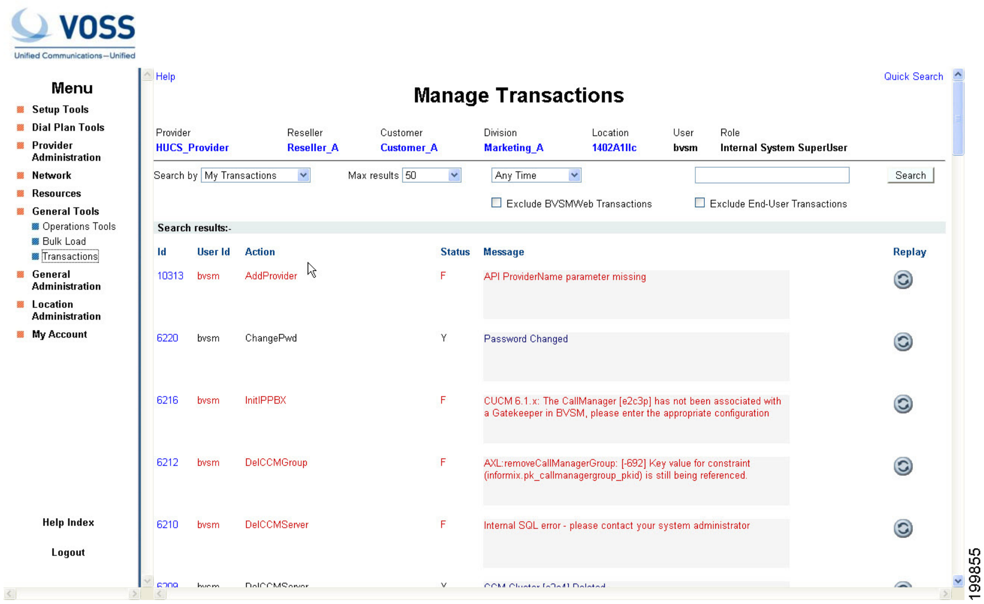
This step is performed at the location level from the User Management page for the location.

5. Log-on to a phone with a Mobility Profile (once logged-on, the phone adopts the user mobility profile). For information about using the Phone Management option, refer to *Customizing Your IP Phone*.

Transactions (General Tools)

Select the **Transaction Option** on the General Tools menu to view a list of transactions on the Hosted UCS system. (see Figure A-3).

Figure A-3 Transactions



Use the Transactions option to view the status of recently completed transactions, such as login attempts and password changes. Use the pull-down selection lists for the following:

- Control the number of results displayed
- Specify a time range
  - Any Time
  - Within Hour
  - Within 24 Hours
- Select the type of criteria to use for searching:
  - Action type
  - Cancelled transactions
  - All transactions

Use the Search field to locate a specific transaction.

Hunt Groups

A hunt group is a set 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 are created by the customer administrator, but you can use the Hunt Groups option to add or remove lines an existing hunt group.

Note Before you can add lines to a hunt group, you must first create the line group, as described in the "Pickup Groups" section on page A-7. A single line group can be used with multiple hunt groups, and multiple line groups can be used with a single hunt group.

Managing Hunt Groups

You can use the **Hunt Groups** option to change the Maximum Hunt Timer, which determines how long an incoming call will ring the line groups associated with the hunt group. You can also use this option to change the Call Forward Destination, which is the number to which the call is forwarded if the call is not answered within the time specified by the Maximum Hunt Timer.

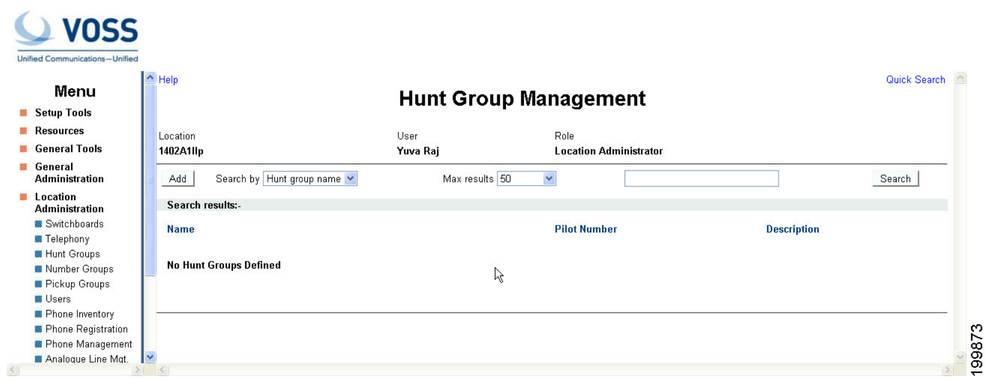
To configure the Maximum Hunt Timer or Call Forward Destination, complete the following steps:

Procedure

Step 1 After creating the associated line groups, select **Hunt Groups** on the Location Administration menu.

The Hunt Group Management page appears (see Figure A-4).

Figure A-4 Hunt Group Management



To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click the link for the hunt group you want to manage in the Name column.
This page displays the configuration of the hunt group that has been completed by the customer administrator, and lets you perform the following operations:

- Select a line group to be used by this hunt group (see the "Managing Lines in a Hunt Group" section on page A-7)
- Change the text description of the hunt group in the Description field.
- Change the number to which the incoming call will be forwarded if it is not picked up by an associated line group within the time specified by the Maximum Hunt Timer.
- Select the number of seconds from the Maximum Hunt Timer pull-down selection list. This timer specifies the total length of time that the incoming call will ring on any associated line groups before it is forwarded to the number specified in the Call Forward Destination field.
- Click the blue link in the Name column of the Line Groups section to display the Line Group Management page for any line group associated with the hunt group.

Step 3 After making any changes necessary (except for adding a line group which requires going to another page), click **Submit**.

Managing Lines in a Hunt Group

Use the **Hunt Groups** option to add or remove line groups to or from an existing hunt group. To add a new hunt group, contact your customer administrator.

To manage the lines in a hunt group, complete the following steps:

Procedure

Step 1 After creating the associated line groups, select **Hunt Groups** on the Location Administration menu.

The Hunt Group Management page appears (see Figure A-4).

Step 2 Click the link for the hunt group you want to manage in the Name column.

Step 3 Click **Select Line Group** to add a line group to the hunt group.

Step 4 Select the order in which the current line group will be called from the Group Order pull-down selection list.
The hunt group forwards the call to the first line group in the list of associated line groups. A line group can be configured to forward the call to another line group when it is not answered in a specified length of time. This option determines the order in which each line group is called.

Step 5 Select the line group from the Line Group Name pull-down selection list.

The Line Group Name pull-down selection list lets you select line groups that have been created using the Line Groups option.

Step 6 Click **Submit**.

Step 7 Click **Return to Hunt Groups**.

Pickup Groups

A pick-up group is a set of phone numbers that allows a user of any phone in the group to answer an incoming call by pressing a soft key button. Pickup groups are created by customer administrators, but Location-level administrators can add or remove numbers from a pickup group or associate and unassociate pickup groups. When two pickup groups are associated, they function as a single pickup group as long as they remain associated.

Group pickup allows the user of a phone that is not in the pickup group to also pick up a call. This is achieved by the use of the Group pickup extension number.

Pickup groups are created by the customer administrator, but you can use the **Pickup Groups** option to manage an existing pickup group.

Adding Numbers to a Pickup Group

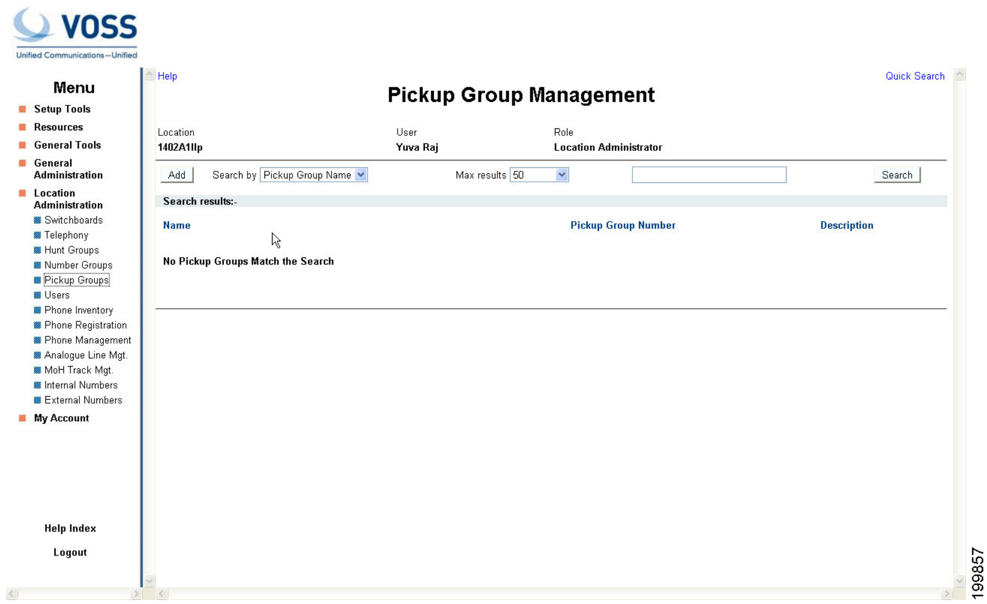
To add numbers to an existing pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

The Pickup Group Management page appears (see Figure A-5).

Figure A-5 Pickup Group Management



To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Select the name of the pickup group on the Pickup Group Management page.

Step 3 Click **Add Number** on the Pickup Group Management page.

Step 4 Select a number to add to the pickup group from the pull-down selection list on the Add Number page.

Step 5 Click **Add.**

To add additional numbers to a pickup group, repeat steps 2 through 5.

Associating Pickup Groups

When two pickup groups are associated, they function as a single pickup group as long as they remain associated.

To associate a pickup group with another pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

Step 2 Select the name of the pickup group on the Pickup Group Management page.

Step 3 Click **Associate**.

Step 4 Select the pickup group to associate with the current pickup group from the Pickup Groups to Associate pull-down selection list.

Step 5 Click **Associate**.

Users

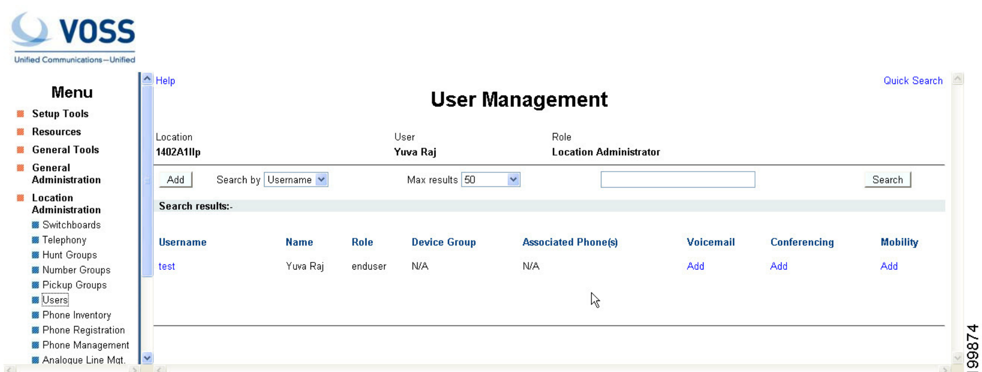
This section describes the following tasks that you can perform using the Users option on the Location Administration menu:

- Adding a User Account, page A-9
- Deleting a User Account, page A-12
- Managing Voice Mail Accounts, page A-10
- Managing Mobility Profiles, page A-11
- Associating and Unassociating a Phone with a User, page A-11

Managing User Accounts

The User Management page (Figure A-6) displays the existing user accounts for the current location. This page lets you add a new user account or select an existing account that you want to manage.

Figure A-6 User Management



To search for a user account, select Username or Surname (last name) from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

To manage an existing user account, click the blue entry in the Username column. A User Account Management page appears on the screen. You can use this page to change the PIN associated with the account, manage the roaming profile, set up a voice mail account, or associate a phone. If the phone is already associated, you can use this page to unassociate the phone. .

Adding a User Account

When you create a user from the Location Administration menu, the user account is added to the central Hosted UCS database, linked to the new location. To add a user account to a different location, you must login to an account linked to that location with Location administrator privileges.

To add a new user account, complete the following steps:

Procedure

Step 1 On the User Management page, click **Add**.

Step 2 Enter the details for the user account in the fields provided.

The username must be an alphanumeric string without spaces that is unique for the entire Hosted UCS system. Adding a short location identifier to each name ensures that the username is unique.

Note Required fields are indicated by a red asterisk (*).

After completing the fields on this page, click **Next**.

Step 3 Enter a PIN number to be associated with the user account.
The Pin code must be a minimum of 5 digits in length.

Step 4 Complete the other fields as required in your location. (Optional)

Step 5 Select the feature group from the pull-down selection list.
A feature group, which specifies the phone features that can be enabled, is defined by the division administrator or customer administrator.

Step 6 Select the access profile to be used to set up the account.

Step 7 Select the BT Enduser Profile to provide standard permissions.

Step 8 Enter the account number to be used for accounting purposes.

Step 9 After completing all the fields required for your location, click **Add**.

The user account is added to the database.

Managing Voice Mail Accounts

IP Voicemail allows callers to leave messages when a phone is unanswered or forwarded for any reason to the Voicemail system. Users can then retrieve their voice messages at their leisure.

Note Before creating a voicemail service within a location, a Voicemail Resource and corresponding Pilot number must be created for the customer by the Provider Administrator.

To create a voice mail account, complete the following steps:

Procedure

Step 1 On the User Management page, click the blue entry in the Username column.

Step 2 On the User Account Management page, click **VoiceMail**.

Step 3 Click **Personal VoiceMail** or **Group VoiceMail** depending on whether you want to create a private voicemail account for the associated user account, or a group voicemail account that can be shared by a number of users.You can also click the **Add** link in the Has VoiceMail or Has Group VoiceMail column on the User Management page to go directly to this page.

Step 4 Enter a password for the user account.

Managing Mobility Profiles

A mobility profile allows a user to log onto a phone in another location and the phone automatically adopts the profile for that user. A mobility profile is required for users who move between locations on a regular basis, or for users in an organization or location that assigns each user a mobility profile rather than a permanent phone.

Note the following when adding a mobility profile to a user account:

- 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 are assigned by the Customer Administrator.

To add a mobility profile to an existing user account, complete the following steps:

Procedure

Step 1 On the User Management page, click the blue entry in the Username column.

Step 2 On the User Account Management page, click **Roaming Profile**.
The Add Mobility Profile page appears, or if the profile already exists, the Manage Mobility Profile page appears.

Step 3 Enter the correct roaming profile numbers for the user and click **Add**.
The Division Administrator or Customer Administrator can use the Hosted UCS bulk loading mechanism to quickly add mobility profiles for a group of users.

Step 4 To delete a mobility profile, click **Delete**.

Associating and Unassociating a Phone with a User

Associating a phone with a user account configures the phone with the user account settings and links the phone to the user account, allowing the user to customize the phone settings. After association, the phone will operate as the phone for the associated user until it is de-registered.

The Division Administrator or Customer Administrator can use the bulk loader utility to automatically process multiple associate commands in one step. Often when setting up a new location the bulk loader is a better way to associate many users to their phones.

When a user account is associated to a phone, two associations are actually created and listed.

The second listing, “not for calls” is for when the phone does not have lines. It is possible to associate a user to a phone which does not have any lines. When the phone as lines, the user account is associated to both the phone and to the first line on the phone.

When associating a phone to a user account, note the following:

- Phones must be associated with the user account at the location level.

- The phone must be available for association with the user account.

To associate a phone with a user account, complete the following steps:

Procedure

Step 1 On the User Management page, click the blue entry in the Username column.

Step 2 On the User Account Management page, click **Phone Associate**.
A list of available phones appears that are not already associated with another user account. Determine which phone has been registered to be associated with the User.

Step 3 Click **Associate** on the same row as the appropriate phone to start the automated configuration of the phone and to associate it with the current user account.

Step 4 Click **Associate Phone**.

Step 5 To unassociate a phone, click **Un-Associate** on the User Management page.

Note To move a user from one location to another, first delete the user account and then recreate the account in the new location. Before deleting the user account, you must un-associate all phones and lines from the account.

Deleting a User Account

To delete a user account, complete the following steps:

Procedure

Step 1 On the User Management page, click the blue entry in the Username column for the account you want to delete.

Step 2 Click **Delete** at the bottom right hand corner of the screen.

Note Deleting a user account provides a transaction record that indicates whether the request was successful or not. If the transaction was unsuccessful, the transaction record may provide an explanation of the problem.

Phone Registration

You need to register and unregister phones when you reallocate phones or add new phones. A new phone must be registered before it can be used. Note the following in regard to registering phones:

- You must register phones for each location.
- A phone must be provisioned for the location before it can be registered.

After a phone is assigned to a location it is assigned its IP address and will appear in the USM database in the Unregistered state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

When the phone is registered, it is assigned a feature group and an external (DDI) number. After registration, the phone can be used for logging in to a Mobility profile, and can be used to make calls to external numbers.

Contact your Customer Administrator or Division Administrator if you need phones to be provisioned.

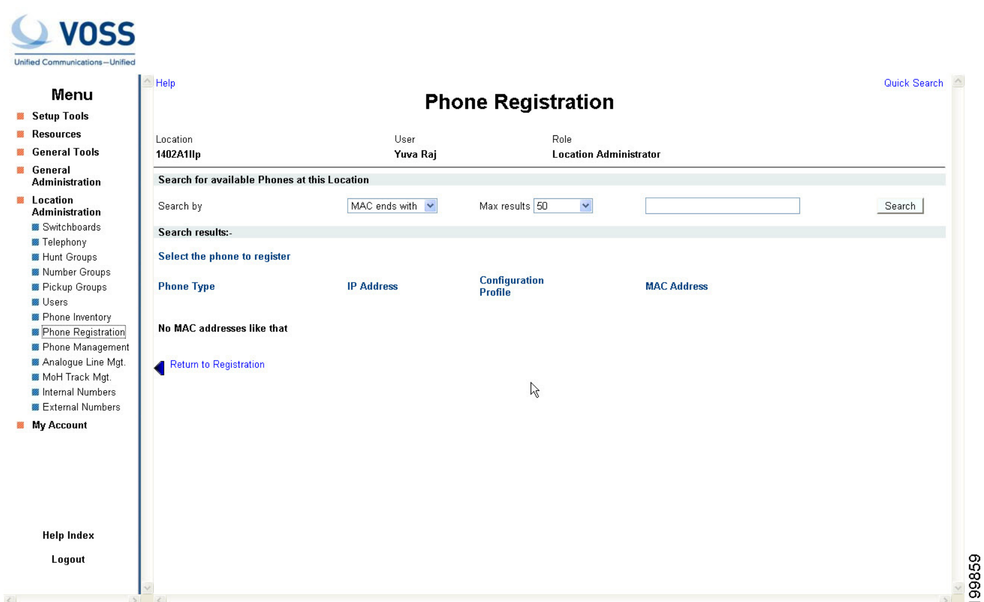
To register a phone, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration menu.

The Phone Registration page appears (Figure A-7).

Figure A-7 Phone Registration



To search for a phone, select MAC ends with or Phone Type from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

This page lists any phones that have been provisioned for your location that are not yet registered.

Step 2 Select the phone you want to register.

Step 3 Select the feature group to use with the phone from the pull-down selection list.

Step 4 Select one or more line numbers from the pull-down selection list that should be associated with the phone.

The number of lines available depends on the model of the IP phone.

Step 5 Click **Register.**
The phone is registered and receives its configuration, dedicated phone numbers (E164, DDI, or extension), feature groups and location. It is now fully operational, but only at its defined location and office subnet.

Phone Management

Note When the call forward options is set using the Services button, the change is synchronized and displayed on the Self Care web page. However, if the call forward option is set using the CFwdALL soft kay, the change is not displayed in the Self Care web pages.

To manage any phone at your location, complete the following steps:

Procedure

Step 1 Select the **Phone Management** option from the Location Administration menu.

Step 2 To search for a phone, select one of the following options from the Search by pull-down selection list:

- MAC starts with
- MAC ends with
- Search by Phone location
- Extension Number Ends with
- Extension Number Starts with
- Full Internal Number

Step 3 Enter as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

This page provides a list of the following information about each phone in the location:

- Phone Type
- Phone MAC address
- Phone First Line Number
- Phone Location
- Associated User

Step 4 To manage a specific phone provisioned at your location, click the blue link in the MAC Address column.
The Phone Management page provides the following options:

- **Phone Status**—View the configuration file on the phone
- **Phone Reset—**Soft boot the phone
- **Logout User—**Logout any user with mobility who may have neglected to log off
- **SpeedDials—**Assign speed dials for the selected phone.

Internal Numbers

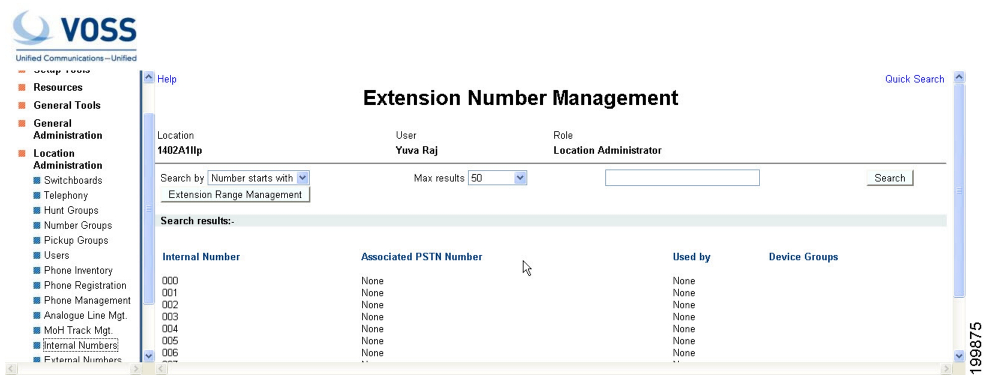
To manage the extensions at your location, complete the following steps:

Procedure

Step 1 Click the **Internal Number** option on the Location Administration menu.

The Extension Number Management page shown in aFigure A-8 appears.

Figure A-8 Manage Available Extensions



The Extension Number Management page lists the extensions assigned to each phone at your location, along with the associated PSTN number.

Step 2 To search for an extension, select one of the following options from the Search by pull-down selection list:

- Number ends with
- Number starts with
- Available

Step 3 Enter as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

APPENDIX B

Hosted Unified Communications Services Division Administration

Revised: 08/12/2010, OL-23270-01

This document describes the options available to Division administrators within the Hosted Unified Communications Services (UCS) system. The options available to the Division administrator depend on the specific Hosted UCS implementation. If you have questions about the availability of a specific option, contact the customer administrator for the Hosted UCS system. The following sections describe the options available to the Division administrator on each submenu:

Overview

This section includes the following topics:

User Interface Guidelines

Note the following conventions used in Hosted UCS menus and associated administration pages:

- Links to other pages are bright blue.
- Required fields are indicated by a red asterisk (*).
- Error messages are displayed in red type.
- Changes to a page are not saved until you click the **Add**, **Submit**, or **Modify** button, which is required to complete the transaction.

- A transaction record generally appears after submitting each change, which indicates if the transaction is successful or if a problem occurred. To view previously completed transactions, use the **Transactions** option on the General Tools menu.
- You can use the browser **Back** button to return to a previously viewed page, or you can click on any option in the navigation menu to go directly to a specific option.

Quick Search

Each page of the USM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries to which you have access are determined by the access privileges associated with the user account that you used to log into the system.

When you click the Quick Search link, the system displays a Quick Search page containing a list of the entries in the Hosted UCS database to which you have access.Select the options described in Table B-1 from the **Search For** pull-down selection list to identify the type of entries for which you want to search.

Click on a blue link on this page to open the management page for the selected entry. To refine your search, select one of the following options from the **Search By** pull-down selection list.

- 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.

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.

Table B-1 Search Types

Search Type	Description
Location Searches	
Location	Find a location by name within the division or customer level.
Location with Site Code	Find a specific location by entering the site code.
Location of User	Find a location by entering a user account name.
Location of Phone	Find a location by entering the Mac address of a phone.
Extension Search	
Extension	Find an extension by its numeric identifier.
Extension associated with DDI	Find an extension by entering the external line to which it is registered.
Extension used by User	Find an extension by entering the associated user account.
Extension used by Phone	Find an extension provisioned on a phone by entering the MAC address of the phone.
Mac Search	
Phone with Mac	Find a phone by entering the MAC address.
Phone with Extension	Find a phone by entering the associated extension.
Phone with DDI	Find a phone by entering the external line to which the phone is registered.

Table B-1 Search Types

Search Type	Description
Phone with User	Find a phone by entering the associated user account name.
User Search	
Username	Find a user account by entering the user account name.
Surname	Find a user account by entering the last name associated with the user account.
Firstname	Find a user account by entering the first name associated with the user account.
User with Extension	Find a user account by entering the extension associated with the user account.

Managing Phones

This section provides an overview of how to manage phones in the Hosted UCS system. It includes the following topics:

- Phone Management Summary, page B-3
- Manually Adding Phones, page B-4
- Removing Phones, page B-4

Phone Management Summary

The following summarizes the tasks for making a new phone available to a user:

1. Add a phone (to the Hosted UCS system).

This is normally accomplished through bulk loading the Mac address, phone type, and associated button template. However, phones can also be added at the Provider Administration level.

2. Move a phone to the location.

This step is performed from the Customer Administration level by moving the phone to a specific location. This associates the phone with the subnet where it gets its IP address assigned. After completing this step, in the USM interface, this phone will appear in an "Unregistered" state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

3. Register a phone (once registered, you can make and receive calls.

This step is performed at the Location Administration level by selecting the phone from a list of unregistered phones in the USM database. On the Phone Registration page for the selected phone, you select the feature group and allocate the DDI line number. This phone then appears in the Registered state in USM.

4. Associate a phone to a user account (once associated, the user account will be listed in the corporate directory).

This step is performed at the location level from the User Management page for the location.

5. Log-on to a phone with a Mobility Profile (once logged-on, the phone adopts the user mobility profile). For information about using the Phone Management option, refer to *Customizing Your IP Phone.*

Manually Adding Phones

A phone can only be added by a service provider administrator and the phone is automatically added at the Provider level, assuming that the phone will physically exist in the provider warehouse. This is normally performed as a Bulk Load process. Once a phone is added to the Hosted UCS system, the MAC address is added to the database and is then tracked by the resource management tools.

Before a phone can be connected to the physical network within a customer location, it must be moved within the Hosted UCS system to the relevant location.

When moving a phone to a location, the Hosted UCS system automatically allocates an IP address to the phone and links it to the phone MAC address within the Hosted UCS system database and the DHCP service.

Once a phone has been moved to a location within the Hosted UCS system, it can be provisioned by physically connecting it to the network. A phone is automatically provisioned by the Hosted UCS system when you connect it to the relevant VLAN, within the correct location. When the phone is provisioned, it will receive an IP address and a default configuration file. It will be operational, but will not allow a user to make or receive calls, other than emergency calls. You will be able to access the menu screens on the phone and confirm the default settings.

If the phone has not been moved into the location within the Hosted UCS system, it will not be allocated an IP address when it is connected to the network. Similarly if you try to connect it to the wrong VLAN it will also not receive its IP address.

Phone registration allocates a Class of Service (CoS) and one or more phone numbers to the phone. Registration involves rebooting the phone by the Hosted UCS system and a new, updated configuration file being sent to the phone. The CoS defines the features and settings that the phone are allocated in its configuration file.

Associating a phone links a user account to a phone, thereby associating that user account with a telephone number. Only one user account can be associated with a single phone. Before association, the phone must be registered with the new CoS and preferences of the user account. The user is not required to log onto the phone.

If the phone CoS has “Phone Extension Mobility” allowed and the user account has a Mobility Profile allocated, then that user can log in to the phone and the phone will adopt the user Mobility profile.

Removing Phones

The process of deleting a phone completely from the system, requires reversing each task in the opposite order in which they were performed when provisioning a phone. For example:

1. Log out, or disassociate the user account from the phone.
2. De-register the phone.
3. Move the phone from the location to the provider (de-provision).
4. Delete the phone from the phone inventory.

Managing Internal and External Numbers

External (or DDI) numbers are unique E.164 numbers that are not necessarily allocated to every business phone. A call from another company can only be placed to an external (DDI) number. You cannot call an internal number from outside the company. Internal numbers are allocated to every phone. They allow internal calls to be made between staff within a company, both intra-location and inter-location. External numbers must be associated to an internal number before it can be registered with a phone, because every phone must have an internal number.

The following summarizes the process of managing numbers:

1. Add E.164 number range.
2. Create internal numbers when adding a location.
3. Move E.164 numbers to a location.
4. Associate E.164 number range to internal number range.
5. Register phone with one or more numbers.

An E.164 number range can only be added by a service provider administrator and the numbers are automatically added at the Provider level, assuming that the numbers have been allocated to the provider by the regulated authority. Once a number range has been added to the Hosted UCS system, the numbers are added to the Hosted UCS system database and are then tracked by the system management tools.

Internal numbers are created automatically when a location is created. Part of the location configuration process requires the number of internal lines to be specified and the Hosted UCS system automatically creates the configured number of internal numbers. Internal numbers can be added by modifying the configuration of a location. Internal numbers are created on the basis of the definitions created in the Dial Plan number construction section. This defines the number of digits in the site code and extension number.

Before an external number can be used by a phone on the physical network within a customer location, it must be moved within the Hosted UCS system to the relevant location. The Hosted UCS system maintains a record of where numbers are allocated.

Once an External Number Range has been moved to a location, it can then be associated with an internal number range. This procedure is performed at the Location level. If the external number range has not been moved into the correct location, it cannot be associated with the internal number range.

When a phone is registered, it is always given an internal number. If the CoS or feature group for the phone allows for an external or DDI number, then it will also receive an external number. You cannot allocate an external or DDI number to a phone if the external number is not associated with an internal number for that location.

Managing Services

Managing services consists of the following major steps:

1. Create Services at the Provider Level (Provider Management).
2. Allocate Services to Customer locations (General Administration).
3. Create and Allocate Services to feature groups (General Administration).
4. Allocate Services to Users (Location Administration).
5. Manage Services in Profile.

Services are created at the Provider level when a provider is created. Part of the provider configuration process requires the number of Services to be defined and the Hosted UCS system automatically creates the configured number of Services. Services can be added to by modifying the service counters within the Provider Management menu.

Before a service can be allocated to a user account within a customer location, it must be moved within the Hosted UCS system to the relevant location. This requires service counters to be increased at each level, including customer, division (if used), and location.

The Hosted UCS system maintains a record of where services are allocated through the service counters at each level. Additional services can be ordered at any one level by modifying the reserved services counters. Changes to service counters can be configured to create billing records, allowing service providers to charge customers when they re-order services.

Feature groups provide the mechanism for packaging services for user accounts. When you create a feature group, you define the services that are authorized for user accounts within that feature group. You cannot authorize services for user accounts any other way.

You allocate the feature group to a user account when you create the user account. This feature group sets the default when creating a mobility profile for the user.

The customer administrator can modify a user account feature group and can modify the underlying services within the feature group.

Once a user account has been allocated a feature group, the services in that feature Group will then be present in their user account profile. For example, if they are allocated the User Mobility service, then the Mobility Profile option will be present on their Manage User page.

Add services to the user account by modifying the User Profile in the Manage User page. Once the service has been added, you can configure the service for that user account. Again, using Mobility as the example, once the service has been added to the user account, the Mobility Profile Configuration link will be present on the Manage User page.

Users can manage their own services on their Self Care pages, using the Manage Profile option. Certain service configuration variables (not all) are available under Self Care for the user to manage. The balance of the service configuration can be managed by the location administrator, using the Manage User page.

If you cannot add a service to a user account, verify the following:

- Does the user account have the correct feature group allocated?
- Does the location have sufficient services available to be allocated to this user account?

If the user account does not have the correct feature group, then you will need to change their feature group. If the location does not have sufficient service resources, then you will need to re-order more resources from their parent company resources.

Resources/Phone Inventory

Note The specific options available on the Resources menu may vary depending on your Hosted UCS implementation.

This section describes the Phone Inventory option on the Resources menu. Phones are added to the Inventory by the provider administrator and allocated to customers. As the customer administrator, you can allocate phones to divisions, locations, and users. The Hosted UCS system tracks the inventory and provides feature management for each phone.

The Phone Inventory option lets you view information about phones, assign a phone to a location, and move a phone between locations.

To view the phone inventory or move a phone between locations, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the Resources Menu.
A Phone Inventory page having a list of the phones on the system with their location and status, is displayed. To search for a phone, select one of the following options from the Search by pull-down selection list:

- MAC starts with
- MAC ends with
- Search by phone location
- Extension Number Ends with
- Extension Number Starts with
- Full Internal Number

Enter as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

Step 2 Click the blue link in the MAC address column to view information about a specific phone or move it to a different location, in the Phone Inventory page.

Step 3 Click **Next**.

Step 4 Select the location to which you want to move the phone from the pull-down selection list, in the Phone Inventory page.

Step 5 Click **Next**.

Step 6 Click **Move Phone**.

The transaction record appears and the phone is moved to the designated location.

General Tools

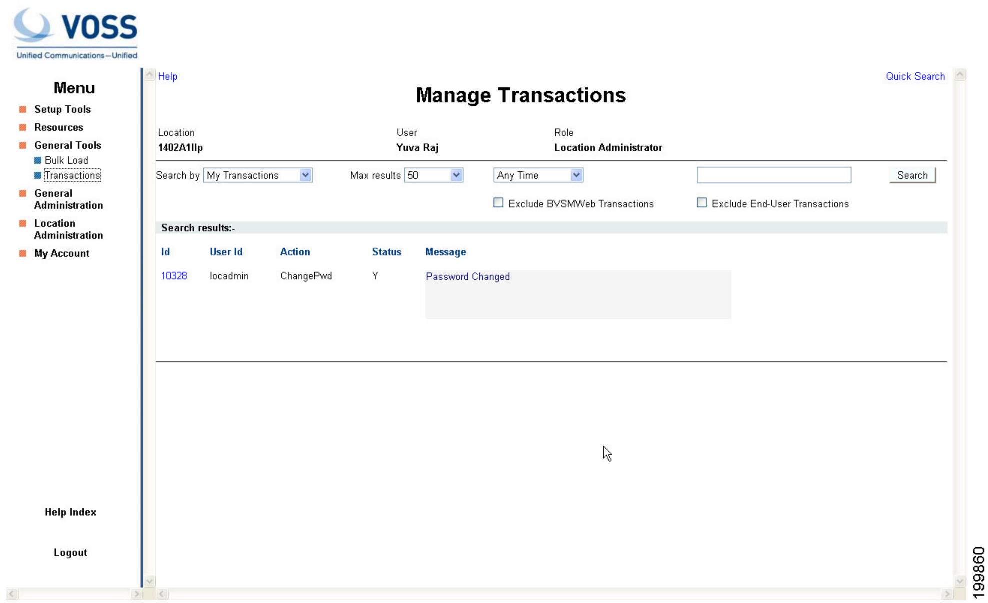
Note The specific options available on the General Tools menu may vary depending on your Hosted UCS implementation.

This section describes the Transaction options on the General Tools menu.

Transactions

Use the **Transactions** option to view the status of recently completed transactions, such administrative changes, user login attempts, and password changes. When you select the **Transactions** option, the screen shown in Figure B-1 appears.

Figure B-1 Manage Transactions



To search for a Transaction, select the appropriate option from the pull-down selection lists to specify the search criteria and click **Search**.

- Specify a time range:
  - Any Time
  - Within Hour
  - Within 24 Hours
- Select the type of criteria to use for searching:
  - Action type
  - Cancelled transactions
  - All transactions)

General Administration

> **Note** The specific options available on the General Administration menu may vary depending on your Hosted UCS implementation.

This section describes the Location option on the General Administration menu.

Locations

When adding a new location, you must first confirm that the following steps have been completed by your service provider:

- The new location has cabling installed within the building and individual offices are connected

- The Cisco ISR or 3600 line-powered switch has been installed on-site at the new location and connected to the service provider network
- The IP Subnet address (or Pool Addresses) have been allocated and the Edge Device has been configured for the IP Subnet
- The E.164 telephone numbers have been allocated
- Phones have been provisioned by the Hosted UCS system, allocated to the new location and are physically available at the new location

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
- Primary location Number (i.e. main number): for example, 86644000
- Emergency Number (for callback by emergency services): for example, 86644001
- Start and end range for E.164 telephone number range to be allocated to users in this location: for example, 86644000 to 86644999
- Phone MAC addresses: for example, 12.34.56.78.AB.90

The following is a summary of the tasks for adding a new location:

1. Add the location details, scope of services and infrastructure configuration the Hosted UCS system automatically configures the Cisco Unified Communications Manager, gatekeepers, transit switch and PSTN Gateway for the new location, and the new location is added to the Hosted UCS database.
2. Add new user details, including their services and features into the Hosted UCS system, including site administrators. The Hosted UCS system creates the users within the central database, linked to the new location.
3. Register the phones, which allows the location phones to be recognized by the Hosted UCS system when they are plugged into their new office locations. The Hosted UCS system configures the Cisco Unified CM and IP management system for the new phones, linking them to their location and IP Subnet.

   Registered phones will be able to acquire an IP address and obtain their configuration file (phone number) and once they have fully booted, will operate as an authorized phone.
4. Associate each phone to the user, which links the user to their phone, allowing them to personalize the phone. The Hosted UCS system links the user to the phone within the central database. The phone will thenceforth operate as the user phone, until the user is disassociated with the phone. The user will be able to personalize the settings of the phone.

Adding a Location

Refer to the following when adding locations:

- A location administrator cannot add a new location. Only division administrators or higher (including customer administrators) are authorized to add locations.
- You must add a location from the Location Management page.
- You must first add the parent customer (and division if used) before adding the location.
- After adding the location, add the associated phones and users.

To add a new location, complete the following steps:

Procedure

Step 1 Select **Location** from the Location Administration menu.
A Location Management page having a list of the locations in the Hosted UCS system, is displayed. You can use this page to search for locations in the database, to manage a specific location, or add a location.

Step 2 To manage an existing location, click the blue link in the Name column.

Step 3 To add a location, click **Add**.
An Add Location screen is displayed.

Step 4 Enter the details required for the current location. The mandatory fields are indicated by a red asterisk in the Add Location screen.

Step 5 Select Hardware Group from the drop-down menu.
Hardware group is very important and defines a set of hardware devices, including PBXs, Transit Switches, and so forth. Through selection of an appropriate Hardware Group you are controlling the set of hardware resources that is assigned to the new location. Obtain this information from your service provider.

Step 6 Click **Next**.

Step 7 Select the site code for the location from the pull-down selection list, in the Add Location page.
The service provider configures the entries on the Site Code pull-down selection list.

Step 8 Select the local area code (prefix to dial this area) for the location.
The service provider configures the entries on the Area Code pull-down selection list.

Step 9 Set the extension number length and outside line prefix.
The service provider configures the options available.

Step 10 Select the IP subnet.
The service provider configures the subnets before creating the location.

Step 11 Select the branding for the location from the Default branding of User Interface pull-down selection list.

Step 12 Click **Add**.

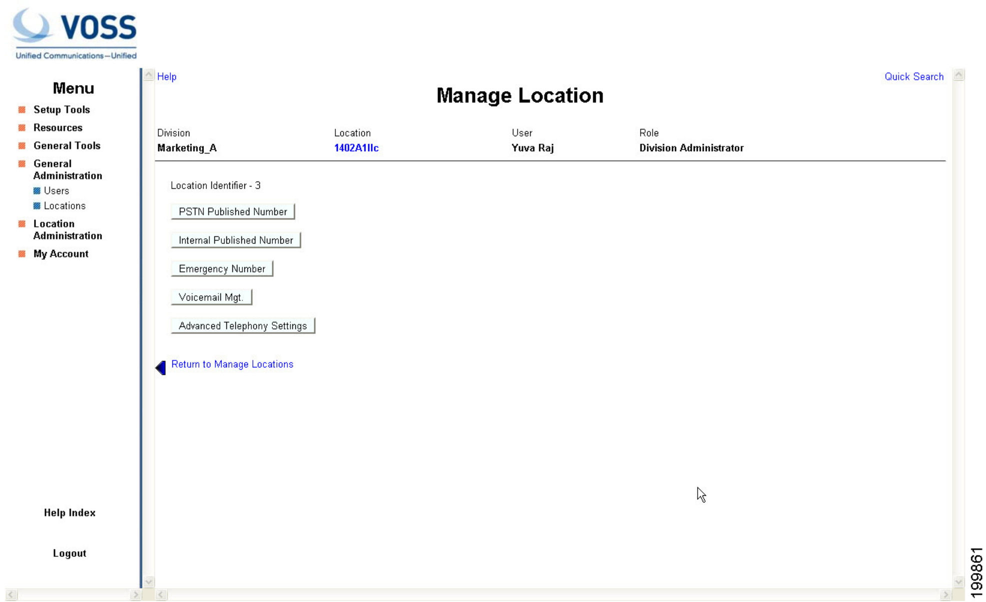
The system starts automatically configuring the new location.

Managing Location Resources

The screen shown in Figure B-2 appears when you click **Advanced Mgt.** on the Manage Location page. This page provides the following options, which are described in the following sections:

- PSTN Published Number
- Internal Published Number
- Emergency Number
- VoiceMail Mgt.
- Advanced Telephony Settings.

Figure B-2 Manage Location



PSTN Published Number

To manage the PSTN numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Advanced Mgmt > PSTN Published Number**.

Step 2 Enter the PSTN number in the Published PSTN Number field.

Note Use the information given on the screen for the format of this number. Otherwise, some calls to the PSTN (such as those from internal numbers) may fail.

Step 3 Click Modify.

Internal Published Number

To manage the internal published numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Advanced Mgmt > Internal Published Number**.

Step 2 Select the internal number to add to the location from the Internal Published Number pull-down selection list.

Step 3 Click **Add**.

Emergency Number

To manage the emergency numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Advanced Mgmt > Emergency Number**.

Step 2 Select the emergency number for the location from the Emergency Number pull-down selection list.

Step 3 Click **Submit**.

VoiceMail Management

To create a voicemail service within a location, the service provider must first create the voicemail resource and corresponding pilot number for the customer that owns the location.

To manage voicemail services, complete the following steps:

Procedure

Step 1 Click **Advanced Mgmt > VoiceMail Mgt**. on the Manage Location page.
A VoiceMail Management page having a list of the voicemail services in the current location, is displayed. You can use this page to search for voicemail services in the database, to manage a specific voicemail service, or add a voicemail service.

Step 2 To manage an existing voicemail account, click the blue link in the Name column.

Step 3 To add a voicemail service, click **Add**.

Step 4 Enter the voicemail service name.

Step 5 Select the voicemail resource from the pull-down selection list.

Step 6 Click **Next**.

Step 7 Select the pilot number from the pull-down selection list.
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 outside the customer to retrieve voicemail messages. The pilot number must be a DDI (E.164) 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 level.

Step 8 Click **Add**, or Click **Add and Enable** to add the voicemail service to the location and make the voicemail service available for all the phones and users already set up or configured at this location.

Advanced Telephony Settings

To manage the Advanced Telephony Settings, do the following:

Procedure:

Step 1 Click **Advanced Mgmt > Advanced Telephony Settings** on the Manage Location page.
An Advanced Telephony Settings page is displayed.

Step 2 Under Details, Select the **Emergency CLI Preference** using the pull-down menu.

Step 3 Click **Submit.**

Location Administration

Note The options available on the Location Administration menu may vary depending on your Hosted UCS implementation.

This section describes the following options on the Location Administration menu.

Switchboards

Refer Location Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Telephony

Refer Location Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Hunt Groups

A hunt group is a set 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 are created by the customer administrator, but you can use the Hunt Groups option to add or remove lines from an existing hunt group.

Note Before you can add lines to a hunt group, you must first create the Number group, as described in the "Number Groups" section on page B-15. A single Number group can be used with multiple hunt groups, and multiple number groups can be used with a single hunt group.

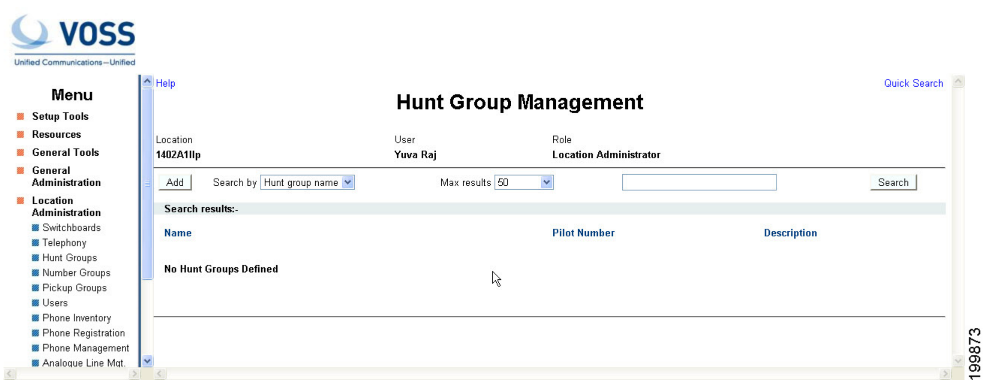
This section describes how to add a hunt group to a location. For information about managing hunt groups, including adding lines to a hunt group, see Appendix A, "Hosted Unified Communications Services Location Administration".

To create a hunt group, complete the following steps:

Procedure

Step 1 Select **Hunt Groups** on the Location Administration menu.
The Hunt Group Management page appears (see Figure B-3).

Figure B-3 Hunt Group Management



To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add**.

Step 3 Enter a unique name for the hunt group.

Step 4 Enter a description for the hunt group (Optional).

Step 5 Select the pilot number from the Pilot Number pull-down selection list.
The pilot number, when called, directs the call to the hunt group.

Step 6 Enter a number to which the call should be directed when it is not answered in the Call Forward Destination field.
Each Number group contains a group of numbers that ring when a call is placed to the specified pilot

number. More than one number group can be associated with a hunt group, which allows the call to roll over to the second number group if no member of the first number group answers the call. If none of the lines associated with any number group answers the call within the time limit specified by the Maximum Hunt Timer pull-down selection list, the call is forwarded to the number specified in the Call Forward Destination field.

Step 7 Select the maximum ring time from the Maximum Hunt Timer pull-down selection list.
Each number group has rules regarding how the call rolls over to the next line or number group, and how long it should ring before rolling over. The Maximum Hunt Timer specifies the total maximum length of time the call can ring on every line in each number group. Therefore this value should either be set high enough, or the RNA Reversion Timeout on the number group should be configured short enough to allow each line to be called before the Maximum Hunt Timer expires.
The maximum length of time that can be set for this timer is 180 seconds (3 minutes).

Step 8 Click **Add** at the bottom of the Add Hunt Group page.

Using a Hunt Group with Multiple Number Groups

You can use a hunt group with a ordered list of number groups that can be used in sequence.

To add a number group to an existing hunt group, complete the following steps:

Procedure

Step 1 On the Hunt Group Management page, select the name of the hunt group to which you wish to add a Number group.

Step 2 Click **Select Number Group.**
The Select Number Group page appears.

Step 3 Select a Number group to add to the Hunt Group from the pull-down selection list.

Note The same number group can be added to more than one hunt group.

Step 4 Select the order in which the Number group should be used.

Step 5 Click **Add**.

Number Groups

A Number group is a set of phones that can be used by one or more hunt groups to determine the way that incoming calls are handled when a call is received by the pilot number assigned to the hunt group.

For instructions about creating a number group, see Appendix A, "Hosted Unified Communications Services Location Administration".

Note Number groups in the location administrator level are called line groups.

Pickup Groups

A pick-up group is a set of phone numbers that allows a user of any phone in the group to answer an incoming call by pressing a soft key button. Pickup groups are created by customer administrators, but location administrators can add or remove numbers from a pickup group or associate and unassociate pickup groups. When two pickup groups are associated, they function as a single pickup group for as long as they remain associated.

Group pickup allows the user of a phone that is not in the pickup group to also pick up a call. This is achieved by the use of the Group pickup extension number.

This section describes how to add a pickup group to a location. For information about managing pickup groups, including adding lines to the pickup group, see Appendix A, "Hosted Unified Communications Services Location Administration".

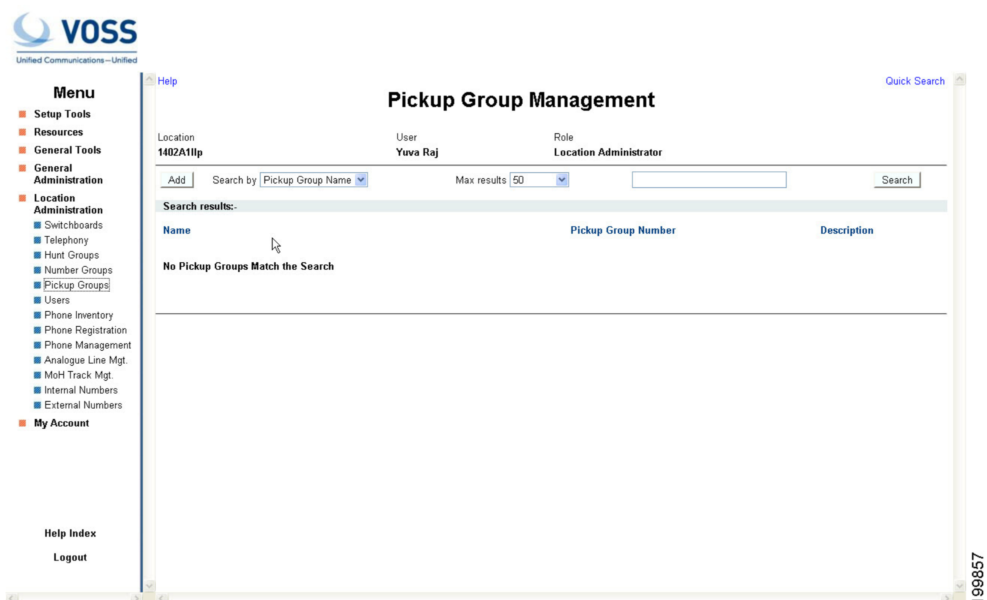
To create a pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

The Pickup Group Management page appears (see Figure B-4).

Figure B-4 Pickup Group Management



To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add** on the Pickup Group Management page.

Step 3 Enter a unique name for the pickup group.

Step 4 Enter a description for the pickup group (Optional).

Step 5 Select a number that is not within the pick-up group that will be allowed to pick up a call.

Step 6 Click **Add**.

Users

This section describes how to change password for users within a location. For information about creating and managing user accounts, refer to Appendix A, "Hosted Unified Communications Services Location Administration".

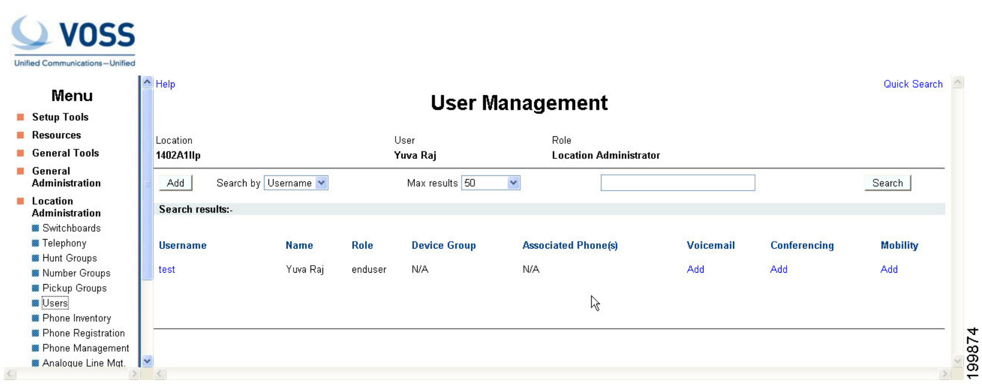
To change the password for a user, complete the following steps:

Procedure

Step 1 Click **User** on the Location Administration menu.

The screen shown in Figure B-5ppears.

Figure B-5 Location/User Management



Step 2 Click the blue link in the Username column for the user account you want to manage.

Step 3 Click **Change Password**.
A Reset Password page appears on the screen.

Step 4 Enter New Password and Re-enter the New Password.

Step 5 Click **Submit**.

Phone Inventory

Refer Location Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Phone Registration

After a phone is assigned to a location it is assigned its IP address and will appear in the USM database in the Unregistered state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

When the phone is registered, it is assigned a feature group and an external (DDI) number. After registration, the phone can be used for logging in to a Mobility profile, and can be used to make calls to external numbers.

Use the **Phone Registration** option on the Location Administration menu to register phones in the current location.

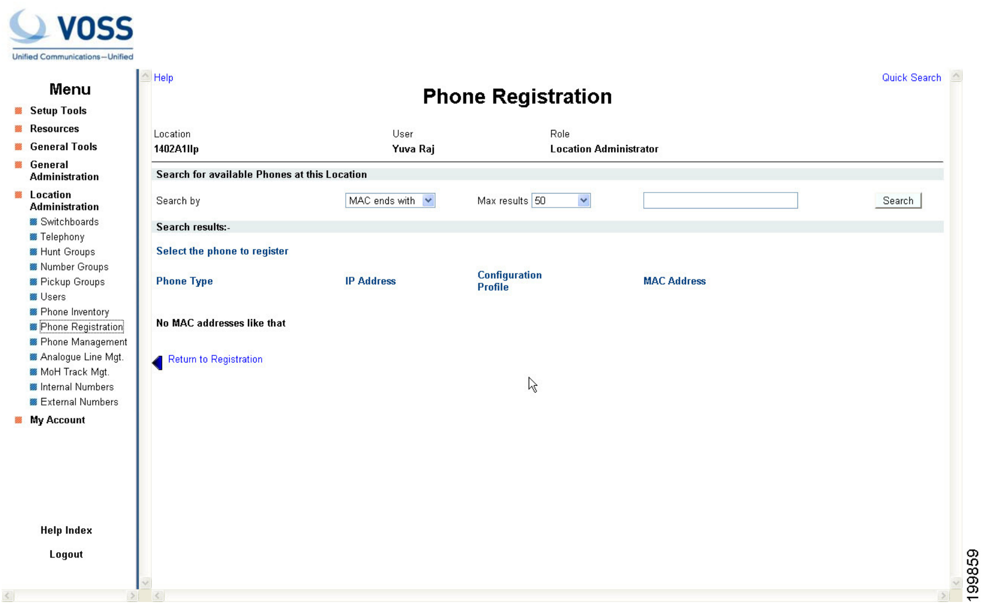
To register phones, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration Menu.

The screen shown in Figure B-6 appears.

Figure B-6 Phone Registration



This page displays a list of the unregistered phones in the current location. You can use this page to search for unregistered phones in the database, to register a specific phone, unregister a phone, or display phone status.

Step 2 To register a phone, click the blue link in the Name column.

For further information about registering phones, see Appendix A, “Location Administration.”

Phone Management

Use the **Phone Management** option on the Location Administration menu to manage the phones within a location. For information about managing phones within a location, see Appendix A, “Hosted Unified Communications Services Location Administration”.

Analogue Line Mgmt

Refer Location Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

MoH Track Mgmt

Refer Location Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Internal Numbers

DDI numbers must be associated with an internal number before allocation. Range association allows a set of external numbers to be linked together with a range of internal numbers. Number association is required to ensure that all DDI numbers assigned to a phone or Mobility profile always have an internal number for internal calls. It is also possible to bulk load the DDI numbers and range association.

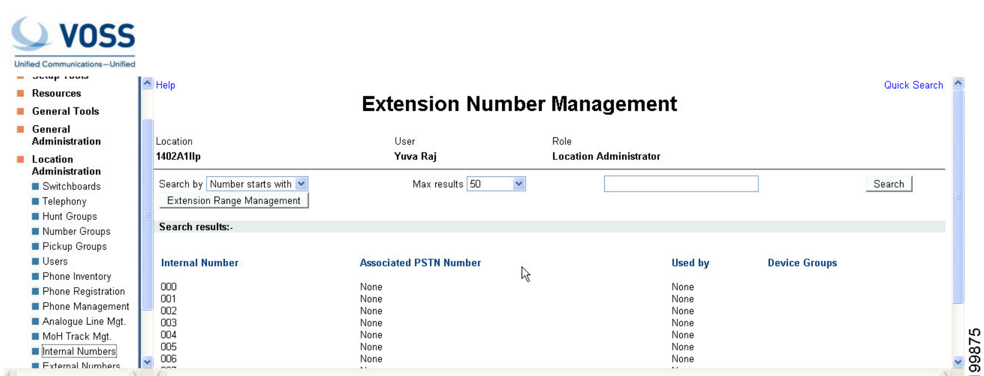
Use the **Internal Numbers** option on the Location Administration menu to manage internal numbers. To manage internal numbers, complete the following steps:

Procedure

Step 1 Select **Internal Numbers** on the Location Administration Menu.

The screen shown in Figure B-7 appears.

Figure B-7 Manage available Internal numbers



The Manage available internal numbers page provides a list of internal numbers, their associated PSTN numbers, their associated phone users, switchboard pilot, and type of phone. You can use this page to search for internal numbers in the database, or to manage the internal number range.

> **Note** You cannot reserve a number if it has already been associated.

Step 2 To manage the internal number range, click **Internal Number Range Mgt.**

Step 3 Enter the starting range for the internal numbers in the Start Internal Number field.

Step 4 Select the number of internal numbers from the Range Size pull-down selection list.

Step 5 Click one of the following buttons, depending on how you want to manage:

- **Enable**—Enable the selected range of internal numbers.
- **Disable**—Disable the selected range of internal numbers.
- **Reserve—**Reserve the selected range of internal numbers.
- **Unreserve—**Unreserve the selected range of internal numbers.

APPENDIX C

Hosted Unified Communications Services Customer Administration

Revised: 08/12/2010, OL-23270-01

This document describes the options available to Customer administrators within the Hosted Unified Communications Services (UCS) system. The options available to the Customer administrator depend on the specific Hosted UCS implementation. If you have questions about the availability of a specific option, contact the Provider administrator for the Hosted UCS system. The following sections describe the options available to the Customer administrator on each submenu:

Overview

This section includes the following topics:

User Interface Guidelines

Note the following conventions used in Hosted UCS menus and associated administration pages:

- Links to other pages are bright blue.

- Required fields are indicated by a red asterisk (*).
- Error messages are displayed in red type.
- Changes to a page are not saved until you click the **Add**, **Submit**, or **Modify** button, which is required to complete the transaction.
- A transaction record generally appears after submitting each change, which indicates if the transaction is successful or if a problem occurred. To view previously completed transactions, use the **Transactions** option on the General Tools menu.
- You can use the browser **Back** button to return to a previously viewed page, or you can click on any option in the navigation menu to go directly to a specific option.

Quick Search

Each page of the USM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries to which you have access are determined by the access privileges associated with the user account that you used to log into the system.

When you click the Quick Search link, the system displays a Quick Search page containing a list of the entries in the Hosted UCS database to which you have access.Select the options described in Table C-1 from the **Search For** pull-down selection list to identify the type of entries for which you want to search.

Click on a blue link on this page to open the management page for the selected entry. To refine your search, select one of the following options from the **Search By** pull-down selection list.

- 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.

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.

Table C-1 Search Types

Search Type	Description
Location Searches	
Location	Find a location by name within the division or customer level.
Location with Site Code	Find a specific location by entering the site code.
Location of User	Find a location by entering a user account name.
Location of Phone	Find a location by entering the Mac address of a phone.
Extension Search	
Extension	Find an extension by its numeric identifier.
Extension associated with DDI	Find an extension by entering the external line to which it is registered.
Extension used by User	Find an extension by entering the associated user account.
Extension used by Phone	Find an extension provisioned on a phone by entering the MAC address of the phone.

Table C-1 Search Types

Search Type	Description
Mac Search	
Phone with Mac	Find a phone by entering the MAC address.
Phone with Extension	Find a phone by entering the associated extension.
Phone with DDI	Find a phone by entering the external line to which the phone is registered.
Phone with User	Find a phone by entering the associated user account name.
User Search	
Username	Find a user account by entering the user account name.
Surname	Find a user account by entering the last name associated with the user account.
Firstname	Find a user account by entering the first name associated with the user account.
User with Extension	Find a user account by entering the extension associated with the user account.

Provisioning Guidelines

The following summarizes the steps required to provision the Hosted UCS system. Many of these steps can be completed using the bulk data loaders (see "Bulk Load" section on page C-11).

1. (Service provider) Creates the customer account and adds the phones to the Hosted UCS phone inventory.
2. (Customer administrator) Creates divisions (if used), locations, and tenants for the customer.
3. (Customer administrator) Creates feature groups.
4. (Customer administrator) Moves the phones to the location.
5. (Location administrator) Creates the user accounts within location.
6. (Location administrator) Registers the phones, assigns phones to feature groups, and associates the phones with user accounts.
7. (Phone user) Logs in to the phone and sets preferences using the Self Care menu or the LCD display on the phone.

Hosted UCS immediately connects the PSTN when you add a location, which prevents verification of the site after installation and prior to cutover. Therefore, it may be better to deploy a location, verify that all the IP phones work within the location, assign all the DDIs, hunt groups, and so forth. After everything is working correctly, connect the telephony service to the PSTN using the **Connect** button on the Manage Telephony page (see the "Telephony" section on page C-18). If the connection to the PSTN fails (for example, the number porting may be incorrect, click **Disconnect**, resolve the issues, and try again.

Managing Phones

This section provides an overview of how to manage phones in the Hosted UCS system. It includes the following topics:

- Phone Management Summary, page C-4
- Manually Adding Phones, page C-4
- Removing Phones, page C-5
- Autoprovisioning, page C-5

Phone Management Summary

The following summarizes the overall tasks for making a new phone available to a user:

1. Add a phone (to the Hosted UCS system).

This is normally accomplished through bulk loading the Mac address, phone type, and associated button template. However, phones can also be added at the Provider Administration level.

2. Move a phone to the location.

This step is performed from the Customer Administration level by moving the phone to a specific location. This associates the phone with the subnet where it gets its IP address assigned. After completing this step, in the USM interface, this phone appears in an "Unregistered" state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

3. Register a phone (once registered, you can make and receive calls.

This step is performed at the Location Administration level by selecting the phone from a list of unregistered phones in the USM database. On the Phone Registration page for the selected phone, you select the feature group and allocate the DDI line number. This phone then appears in the Registered state in USM.

4. Associate a phone to a user account (once associated, the user account is listed in the corporate directory).

This step is performed at the location level from the User Management page for the location.

5. Log-on to a phone with a Mobility Profile (once logged-on, the phone adopts the user mobility profile). For information about using the Phone Management option, refer to *Customizing Your IP Phone*.

Manually Adding Phones

A phone can only be added by a service provider administrator and the phone is automatically added at the Provider level, assuming that the phone physically exists in the provider warehouse. This is normally performed as a Bulk Load process. Once a phone is added to the Hosted UCS system, the MAC address is added to the database and is then tracked by the resource management tools.

Before a phone can be connected to the physical network within a customer location, it must be moved within the Hosted UCS system to the relevant location.

When moving a phone to a location, the Hosted UCS system automatically allocates an IP address to the phone and links it to the phone MAC address within the Hosted UCS system database and the DHCP service.

Once a phone has been moved to a location within the Hosted UCS system, it can be provisioned by physically connecting it to the network. A phone is automatically provisioned by the Hosted UCS system when you connect it to the relevant VLAN, within the correct location. When the phone is provisioned, it receives an IP address and a default configuration file. It is operational, but does not allow a user to make or receive calls, other than emergency calls. You can then access the menu screens on the phone and confirm the default settings.

If the phone has not been moved into the location within the Hosted UCS system, it is not allocated an IP address when it is connected to the network. Similarly if you try to connect it to the wrong VLAN it also does not receive its IP address.

Phone registration allocates a Class of Service (CoS) and one or more phone numbers to the phone. Registration involves rebooting the phone by the Hosted UCS system and a new, updated configuration file being sent to the phone. The CoS defines the features and settings that the phone are allocated in its configuration file.

Associating a phone links a user account to a phone, thereby associating that user account with a telephone number. Only one user account can be associated with a single phone. Before association, the phone must be registered with the new CoS and preferences of the user account. The user is not required to log onto the phone.

If the phone CoS has “Phone Extension Mobility” allowed and the user account has a Mobility Profile allocated, then that user can log in to the phone and the phone adopts the user Mobility profile.

Removing Phones

The process of deleting a phone completely from the system, requires reversing each step in the opposite order in which they were performed. For example:

1. Log out, or disassociate the user account from the phone.
2. De-register the phone.
3. Move the phone from the location to the provider (de-provision).
4. Delete the phone from the phone inventory.

Autoprovisioning

The Hosted UCS system can automate the process of moving the phone to the location, provisioning, and registration. Phones must already be added to the phone inventory and preferences must be set for the customer and location must have been set to permit Autoprovisioning and to define the appropriate business rules, such as default the feature group and number range.

Once a phone is connected to a location network, the Hosted UCS system auto-discovers the phone and the relevant IP Subnet that it is connected to. Once the Hosted UCS system confirms that the phone MAC address is in the known pool of MAC addresses, it automatically assigns the phone to the correct location (IP Subnet) within the Hosted UCS system. The Hosted UCS system then triggers the DHCP server to issue an IP address, which allows the phone to obtain its configuration file. Once a phone is provisioned, you can use the Services button on the phone to confirm autoregistration.

The Hosted UCS system applies a default feature group and selects the lowest number from the internal number pool (with associated DDI if appropriate) to register the phone. The result is that an approved phone can be connected to any office within the correct location and the phones are automatically provisioned and register with a phone number, so that calls can be made to and from the phone.

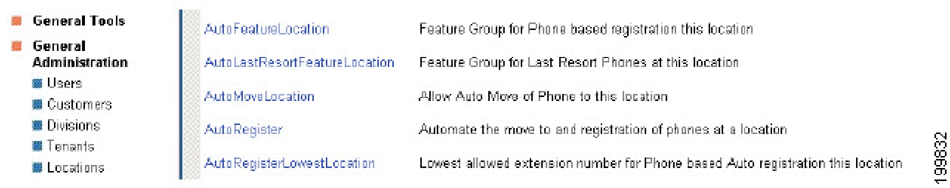
Autoprovisioning can be used by customer administrators for mass rollouts to reduce deployment resources and risk of errors. The customer administrator can also use bulk loaders for the same purpose.

Autoprovisioning may be enabled or disabled at a global, regional or local level. Default number pools and class of service can be defined. Autoprovisioning must be enabled at both Customer and Location levels. In each case, Autoprovisioning is enabled or disabled for the global set of levels under the enabling level.

There are four customer settings for Autoprovisioning. These settings must be set by the provider administrator when the customer is created.

There are five Location settings for Autoprovisioning, as shown in Figure C-1

Figure C-1 Location Preferences for Autoprovisioning



To display these settings, click **Preferences** on the Location Management page (see the "Locations" section on page C-14). The location settings override the customer settings, but both customer and location settings must be set correctly for Autoprovisioning to occur. For example, if the AutoMoveCustomer setting is set to true, but the AutoMoveLocation setting is False, Autoprovisioning is not permitted for that Location.

The following summarizes the Autoprovisioning process:

1. IP Phones are added to USM Inventory and are assigned to a Reseller/Channel (and optionally to the Customer and/or Division levels).
2. A phone is valid for Autoprovisioning if the phone is assigned to a relevant Reseller, Customer or Division, as a parent to the Location. If the Phone is already assigned to a Location, then it has already been provisioned by USM. A Phone is not valid for Autoprovisioning, if it is still in Provider inventory, or is in the unassigned status.
3. The Location and Customer preference settings should be set to true and default settings should be entered.
4. On connection to a Location Voice VLAN switch port, the IP phone sends DHCP Discover/DHCP Request messages to the Hosted UCS Voice-DHCP server identified by the Voice IP Helper Addresses configured for the Voice VLAN.
5. The Voice-DHCP server responds to the DHCP Request message as follows:
   - Previously registered (valid) phones receives an IP address and associated DHCP options
   - Unregistered/Valid and Non-Valid phones are discovered and processed
   - The DHCP server detects the IP address of the edge-router forwarding the DHCP request
   - The DHCP server queries the USM server (providing the MAC address of the phone and IP address of the edge router)
   - USM identifies the location of the phone by reference to the list of IP addresses loaded into USM for valid Edge Routers/Subnets. These Edge Router IP addresses must be unique to a given subnet, in order to cater for Locations which have multiple subnets) if the phone is valid for Autoprovisioning, and if Autoprovisioning is enabled at the location.
   - USM moves the phone to the phone inventory to the required location, assign an IP address to the phone in the appropriate subnet, and configure the DHCP server to provide the relevant DHCP acknowledgement.

- USM also provisions the IP phone as an Unregistered device in the (CCM) IPPBX associated with the location. If the phone is not valid for Autoprovisioning, or if Autoprovisioning is not enabled at the location, USM does not configure the DHCP server and the phone does not receive a valid DHCP acknowledgement.

6. Following successful Autoprovisioning, the IP phone receives a valid IP address for its local subnet, receives the address of the relevant Unified CM TFTP server in its DHCP options and then registers with the relevant CCM IPPBX Subscriber server. The phone shows Unregistered in the Phone Mask and an internal only extension number on the first phone line.
7. If a default feature group is set in the AutoFeatureLocation preference and the default phone number pools set in the AutoRegisterLowestLocation preference, then the phone also automatically registers with the respective default settings. Telephone calls can then be made on the registered phone.
8. A Phone of Last Resort capability is provided by USMUSM. 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.
9. USM can also automatically allocate the registered phone to a predetermined Pickup Group. If the XML-AutoPickupGroupName setting is enabled, then the registered phone is automatically added to the default pick-up group.

The Autoprovisioning process does not provide a regular transaction screen like other transactions. This is because Autoprovisioning runs in the background and is triggered only by a new, valid phone being connected to a location. USM does, however, capture the Autoprovisioning transaction in the transaction logs, available from the General Tools menu.

Managing Internal and External Numbers

External (or DDI) numbers are unique E.164 numbers that are not necessarily allocated to every business phone. A call from another company can only be placed to an external (DDI) number. You cannot call an internal number from outside the company. Internal numbers are allocated to every phone. They allow internal calls to be made between staff within a company, both intra- and inter-location. External numbers must be associated to an internal number before it can be registered with a phone, because every phone must have an internal number.

The following summarizes the process of managing numbers:

1. Add E.164 number range.
2. Create internal numbers when adding a location.
3. Move E.164 numbers to a location.
4. Associate E.164 number range to internal number range.
5. Register phone with one or more numbers.

An E.164 number range can only be added by a service provider administrator and the numbers are automatically added at the Provider level, assuming that the numbers have been allocated to the provider by the regulated authority. Once a number range has been added to the Hosted UCS system, the numbers are added to the Hosted UCS system database and are then tracked by the system management tools.

Internal numbers are created automatically when a location is created. Part of the location configuration process requires the number of internal lines to be specified and the Hosted UCS system automatically creates the configured number of internal numbers. Internal numbers can be added by modifying the configuration of a location. Internal numbers are created on the basis of the definitions created in the Dial Plan number construction section. This defines the number of digits in the site code and extension number.

Before an external number can be used by a phone on the physical network within a customer location, it must be moved within the Hosted UCS system to the relevant location. The Hosted UCS system maintains a record of where numbers are allocated.

Once an External Number Range has been moved to a location, it can then be associated with an internal number range. This procedure is performed at the Location level. If the external number range has not been moved into the correct location, it cannot be associated with the internal number range.

When a phone is registered, it is always given an internal number. If the CoS or feature group for the phone allows for an external or DDI number, then it also receives an external number. You cannot allocate an external or DDI number to a phone if the external number is not associated with an internal number for that location.

Managing Services

Managing services consists of the following major tasks:

1. Create Services at the Provider Level (Provider Management).
2. Allocate Services to Customer locations (General Administration).
3. Create and Allocate Services to feature groups (General Administration).
4. Allocate Services to Users (Location Administration).
5. Manage Services in Profile.

Services are created at the Provider level when a provider is created. Part of the provider configuration process requires the number of Services to be defined and the Hosted UCS system automatically creates the configured number of Services. Services can be added to by modifying the service counters within the Provider Management menu.

Before a service can be allocated to a user account within a customer location, it must be moved within the Hosted UCS system to the relevant location. This requires service counters to be increased at each level, including customer, division (if used), and location.

For information about incrementing service counters at each level refer to <$xref>.

The Hosted UCS system maintains a record of where services are allocated through the service counters at each level. Additional services can be ordered at any one level by modifying the reserved services counters. Changes to service counters can be configured to create billing records, allowing service providers to charge customers when they re-order services.

Feature groups provide the mechanism for packaging services for user accounts. When you create a feature group, you define the services that are authorized for user accounts within that feature group. You cannot authorize services for user accounts any other way.

You allocate the feature group to a user account when you create the user account.

The customer administrator can modify a user account feature group and you can modify the underlying services within a feature group.

Once a user account has been allocated a feature group, the services in that feature group are present in their user account profile. For example, if they are allocated the User Mobility service, then the Mobility Profile option is present on their Manage User page.

Add services to the user account by modifying the User Profile in the Manage User page. Once the service has been added, you can configure the service for that user account. Again, using Mobility as the example, once the service has been added to the user account, the Mobility Profile Configuration link is present on the Manage User page.

Users can manage their own services on their Self Care pages, using the Manage Profile option. Certain service configuration variables (not all) are available under Self Care for the user to manage. The balance of the service configuration can be managed by the location administrator, using the Manage User page.

If you cannot add a service to a user account, verify the following:

- Does the user account have the correct feature group allocated?
- Does the location have sufficient services available to be allocated to this user account?

If the user account does not have the correct feature group, then you must change their feature group. If the location does not have sufficient service resources, then you need to re-order more resources from their parent company resources.

Using the Pilot Number

The pilot number is the primary identifier required when creating a customer within the IP Unity system. The Hosted UCS system ensures that the pilot number is unique for each customer. The pilot number is a unique identifier of the service within the network but also allows users to call the voicemail system to retrieve messages associated with their account (line number). The pilot number is created within the voicemail resource pages, but follows the standard E.164 number management process. The Hosted UCS internal number scheme (14 digit – CPID/RID/Sitecode/Ext) ensures that the pilot number remains unique, even when the same site code (999) and extension number are chosen by different customers.

Setup Tools

Note The specific options available on this menu may vary depending on your Hosted UCS implementation.

This section describes Bulk Loads Samples option in the Setup Tools menu:

Bulk Load Samples

To view sample data used with the **Bulk Load** option for automated provisioning of phones and other resources, select the **Samples** option on the Setup Tools menu.

Note For further details refer Chapter 3, Getting Started with Cisco Hosted Unified Communication Servicers Release 7.1(a)

Provider Administration/Feature Templates

Note The specific options available on the Provider menu may vary depending on your Hosted UCS implementation.

This section describes the **Feature Templates** option on the Provider menu, which lets you configure templates that are used for managing the features available to different groups or phones or locations.

Feature groups provide the mechanism for packaging services for user accounts. When you create a feature group, you define the services that are authorized for user accounts to which the feature group is assigned.

A feature group template provides the features that are enabled by default when creating a new feature group. This makes it easier to maintain consistency among feature groups for different locations. You can then modify the feature group to enable or disable specific features for the location.

To create a feature group, complete the following steps:

Procedure

Step 1 Click **Feature Templates** on the Provider Administration menu.

Step 2 To create a feature group template, click **Add**.

Step 3 Enable or disable each feature that you want to include or exclude from the feature group template.

Step 4 Click **Modify**.

Resources/Phone Inventory

Note The specific options available on the Resources menu may vary depending on your Hosted UCS implementation.

This section describes the Phone Inventory option on the Resources menu. Phones are added to the Inventory by the provider administrator and allocated to customers. As the customer administrator, you can allocate phones to divisions, locations, and users. The Hosted UCS system tracks the inventory and provides feature management for each phone.

The Phone Inventory option lets you view information about phones, assign a phone to a location, and move a phone between locations.

To view the phone inventory or move a phone between locations, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the Resources Menu.
A Phone Inventory page having a list of the phones on the system with their location and status, is displayed. To search for a phone, select one of the following options from the Search by pull-down selection list:

- MAC starts with
- MAC ends with
- Search by phone location
- Extension Number Ends with
- Extension Number Starts with
- Full Internal Number

Enter as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

Step 2 Click the blue link in the MAC address column to view information about a specific phone or move it to a different location.

Step 3 Click **Next**.

Step 4 Select the location to which you want to move the phone from the pull-down selection list.

Step 5 Click **Next**.

Step 6 Click **Move Phone**.

The transaction record appears and the phone is moved to the designated location.

General Tools

Note The specific options available on the General Tools menu may vary depending on your Hosted UCS implementation.

This section describes the following options on the General Tools menu.

- Bulk Load, page C-11
- Transactions, page C-11

Bulk Load

Use the Bulk Load Tools option to use a bulk data loader for importing data into the Hosted UCS system. A bulk data loader is an Excel spreadsheet that follows a strict format that allows information to be automatically loaded to the Hosted UCS system.

The following bulk loaders are provided with the Hosted UCS platform:

- Dial plan model loaders—Including settings for USM, and dial plans for Cisco PGW, and Cisco Unified Communications (Unified CM)
- Configuration loaders—Provider, network, and reseller settings

Note For further details refer the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Transactions

Use the **Transactions** option to view the status of recently completed transactions, such administrative changes, user login attempts, and password changes. When you select the **Transactions** option, the Manage Transaction page appears on the screen.

To search for a Transaction, select the appropriate option from the pull-down selection lists to specify the search criteria and click **Search**.

- Specify a time range:
  - Any Time
  - Within Hour
  - Within 24 Hours
- Select the type of criteria to use for searching:
  - Action type
  - Cancelled transactions
  - All transactions

General Administration

Note The specific options available on the General Administration menu may vary depending on your Hosted UCS implementation.

This section describes the following options on the General Administration menu.

Users

This section describes how to manage users across locations. User accounts are added within a location, using the **Users** option on the Location Administration menu. For information about creating and managing user accounts, refer to Appendix A, “Location Administration.” To change permissions for users within a location, refer to the “Users” section on page C-20.

Use the **Users** option on the General Administration menu to view information about users across locations.

Resellers

Refer General Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Buildings

Refer General Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Customers

Refer General Administration Options in Chapter 3 of the Getting Started with Cisco Hosted Unified Communication Services Release 7.1(a) guide.

Divisions

Use the **Divisions** option on the General Administration menu to manage existing divisions or to add a new division. Divisions are used to group a large number of locations to simply management of a very large number of locations. Each customer must have at least one division to add a location. There is no specific prerequisite information, other than the address and contact details, to add a division.

To manage divisions, complete the following steps:

Procedure

Step 1 Select **Division** on the General Administration Menu.
A Division Management page containing a list of the divisions in the Hosted UCS system, is displayed. You can use this page to search for divisions in the database, to manage a specific division, or add a division.

> **Note** If the Division Management page does not appear immediately, click the links on each page until it appears.

Step 2 To manage an existing division, click the blue link in the Name column.

Step 3 To add a division, click **Add**.

Step 4 Complete any fields required.

Step 5 Set the value of the Increase/Decrease Reservation field to identify the number of phones to allocate of each type for the current division.

The number of phones available for the division are listed in the Available From Parent column. These phones are allocated by the provider administrator to the customer. As the customer administrator, you can increase or decrease the number of phones of each type that you want to assign to the current division.

Step 6 Set the value of the Increase/Decrease Reservation field to identify the number of services to allocate of each type for the current division.

The number of services available for the division are listed in the Available From Parent column. These services are allocated by the provider administrator to the customer. As the customer administrator, you can increase or decrease the number of services of each type that you want to assign to the current division.

Step 7 Select the GUI branding option from the pull-down selection list.

Step 8 Click **Modify**.

The division is added to the database.

Locations

When adding a new location, you must first confirm that the following tasks have been completed by your service provider:

- The new location has cabling installed within the building and individual offices are connected
- The Cisco ISR or 3600 line-powered switch has been installed on-site at the new location and connected to the service provider network
- The IP Subnet address (or Pool Addresses) have been allocated and the Edge Device has been configured for the IP Subnet
- The E.164 telephone numbers have been allocated
- Phones have been provisioned by the Hosted UCS system, allocated to the new location and are physically available at the new location

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
- Primary location Number (i.e. main number): for example, 86644000
- Emergency Number (for callback by emergency services): for example, 86644001
- Start and end range for E.164 telephone number range to be allocated to users in this location: for example, 86644000 to 86644999
- Phone MAC addresses: for example, 12.34.56.78.AB.90

The following is a summary of the tasks required to add a new location:

1. Add the location details, scope of services and infrastructure configuration the Hosted UCS system automatically configures the Cisco Unified Communications Manager, gatekeepers, transit switch and PSTN Gateway for the new location, and the new location is added to the Hosted UCS database.
2. Add new user details, including their services and features into the Hosted UCS system, including site administrators. The Hosted UCS system creates the users within the central database, linked to the new location.
3. Register the phones, which allows the location phones to be recognized by the Hosted UCS system when they are plugged into their new office locations. The Hosted UCS system configures the Cisco Unified CM and IP management system for the new phones, linking them to their location and IP Subnet.

   Registered phones can acquire an IP address and obtain their configuration file (phone number) and once they have fully booted, operate as an authorized phone.
4. Associate each phone to the user, which links the user to their phone, allowing them to personalize the phone. The Hosted UCS system links the user to the phone within the central database. The phone operates as the user phone, until the user is disassociated with the phone. The user can personalize the settings of the phone. If the user logs in, the phone can access their settings/services, such as their Personal Directory.

Adding a Location

Note the following when adding locations:

- A location administrator cannot add a new location. Only division administrators or higher (including customer administrators) are authorized to add locations.
- You must add a location from the Location Management page.
- You must first add the parent customer (and division if used) before adding the location.
- After adding the location, add the associated phones and users.

To add a new location, complete the following steps:

Procedure

Step 1 Select **Location** from the Location Administration menu.
A Location Management page containing a list of the locations in the Hosted UCS system, is displayed. You can use this page to search for locations in the database, to manage a specific location, or add a location.

Step 2 To manage an existing location, click the blue link in the Name column.

Step 3 To add a location, click **Add**.

Step 4 Enter the details required for the current location.
The mandatory fields are indicated by a red asterisk.

Step 5 Select Hardware Group from the drop-down menu.

Hardware group is very important and defines a set of hardware devices, including PBXs, Transit Switches, and so forth. Through selection of an appropriate Hardware Group you are controlling the set of hardware resources that is assigned to the new location. Obtain this information from your service provider.

Step 6 Click **Next**.

Step 7 Select the site code for the location from the pull-down selection list.
The service provider configures the entries on the Site Code pull-down selection list.

Step 8 Select the local area code (prefix to dial this area) for the location.
The service provider configures the entries on the Area Code pull-down selection list.

Step 9 Set the extension number length and outside line prefix.
The service provider configures the options available.

Step 10 Select the IP subnet.
The service provider configures the subnets before creating the location.

Step 11 Select the branding for the location from the Default branding of User Interface pull-down selection list.

Step 12 Click **Add**.

The system begins automatically configuring the new location.

Managing Location Resources

Refer Managing Location Resources, page B-10, Hosted Unified Communication Services Division Administration, Appendix B.

Feature Groups

Feature Groups are the primary means for managing user services. Feature groups are customized by the customer administrator. There are two types of feature groups:

- Feature groups for user accounts
- Feature groups for phones

User-based feature groups define the features, services and usage rights that are assigned to every user mobility profile assigned to the feature group. Phone-based feature groups define the features, services and usage rights that are assigned to each phone in the group.

Feature groups define a set of services, including Class of Service (CoS) to be allocated to a user or a phone. Understanding feature groups and refining their use can significantly improve user experience of IP telephony. Poor feature group definition may result in poor service definition to users and phones.

Configure your feature groups during initial set-up of the Hosted UCS system. Once established, you must add new feature groups when changes to your business occur, such as new services are added, or a new class of service is added.

Feature groups are attached to many user accounts and phones. A change to a feature group may not be relevant to every user account or phone.

Feature groups are created at the Customer level and are common among locations for the customer. Each customer or tenant must create their own feature groups. You must be a customer administrator, or higher, to create or delete a feature group.

To manage feature groups, complete the following steps:

Procedure

Step 1 Select **Feature Groups** on the Location Administration menu.
A Feature Group Management page containing a list of the feature groups in the Hosted UCS system, is displayed. You can use this page to search for feature groups in the database, to manage a specific feature group, or add a feature group.

Step 2 To manage an existing feature group, click the blue link in the Name column.

Step 3 To add a feature group, click **Add**.

Step 4 To enable or disable a feature in the feature group for the customer, check or uncheck the associated checkbox.

Step 5 After selecting the correct set of features, click **Modify**.

Note You can modify a feature group, but use caution because this changes the feature group settings for all the phones and users using that feature group and might impact other locations.

Location Administration

> **Note** The options available on the Location Administration menu may vary depending on your Hosted UCS implementation.

This section describes the following options on the Location Administration menu.

- Switchboards, page C-17
- Telephony, page C-18
- Hunt Groups, page C-18
- Number Groups, page C-19
- Pickup Groups, page C-20
- Users, page C-20
- Phone Inventory, page C-21
- Phone Registration, page C-21
- Phone Management, page C-22
- Analogue Line Mgt., page C-22
- MoH Track Mgt Option, page C-22
- Internal Numbers, page C-23
- External Numbers, page C-24

Switchboards

Use the **Switchboards** option on the Location Administration menu to manage existing switchboards or to create a new switchboard.

To manage switchboards, complete the following steps:

Procedure

Step 1 Select **Switchboards** on the Location Administration Menu.
A SwitchBoard Management page containing a list of the switchboards in the current location, is displayed. You can use this page to search for switchboards in the database, to manage a specific switchboard, or add a switchboard.

Step 2 To manage an existing switchboard, click the blue link in the Name column.

Step 3 To add a switchboard, click **Add**.

Step 4 Enter the information required for the switchboard in the current location

Step 5 Select the options required to configure the switchboard from the pull-down selection lists.

Step 6 Click Add.

Telephony

The **Telephony** option on the Location Administration menu lets you manage phones in the current location.

To manage telephony services for the location, complete the following steps:

Procedure

Step 1 Click the **Telephony** option on the Location Administration menu.

Step 2 A Telephony Management page appears on the screen.

Step 3 To manage the telephony services click **Telephony**.

Step 4 To connect the telephony service, click **Connect**.

Step 5 To add a Call Park service, click **Add**.

Step 6 Click **Submit**.

Hunt Groups

A hunt group is a set 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 are created by the customer administrator, but you can use the Hunt Groups option to add or remove lines an existing hunt group.

Note Before you can add lines to a hunt group, you must first create the Number group, as described in the "Number Groups" section on page C-19. A single Number group can be used with multiple hunt groups, and multiple line groups can be used with a single hunt group.

This section describes how to add a hunt group to a location. For information about managing hunt groups, including adding lines to a hunt group, see Appendix A, "Location Administration."

To create a hunt group, complete the following steps:

Procedure

Step 1 Select **Hunt Groups** on the Location Administration menu.

Step 2 To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 3 Click **Add**.

Step 4 Click **Add** to add a new hunt group.

Step 5 Enter a unique name for the hunt group.

Step 6 Enter a description for the hunt group. (optional)

Step 7 Select the pilot number from the Pilot Number pull-down selection list.
The pilot number, when called, directs the call to the hunt group.

Step 8 Enter a number to which the call should be directed when it is not answered in the Call Forward Destination field.
Each Number group contains a group of numbers that ring when a call is placed to the specified pilot number. More than one line group can be associated with a hunt group, which allows the call to roll over to the second line group if no member of the first line group answers the call. If none of the lines associated with any line group answers the call within the time limit specified by the Maximum Hunt Timer pull-down selection list, the call is forwarded to the number specified in the Call Forward Destination field.

Step 9 Select the maximum ring time from the Maximum Hunt Timer pull-down selection list.
Each line group has rules regarding how the call rolls over to the next line or line group, and how long it should ring before rolling over. The Maximum Hunt Timer specifies the total maximum length of time the call can ring on every line in each line group. Therefore this value should either be set high enough, or the RNA Reversion Timeout on the line group should be configured short enough to allow each line to be called before the Maximum Hunt Timer expires. The maximum length of time that can be set for this timer is 180 seconds (3 minutes).

Step 10 Click **Add** at the bottom of the Add Hunt Group page.

Using a Hunt Group with Multiple Line Groups

You can use a hunt group with a ordered list of Number groups that can be used in sequence.

To add a Number group to an existing hunt group, complete the following steps:

Procedure

Step 1 On the Hunt Group Management page, select the name of the hunt group to which you wish to add a Number group.

Step 2 Click **Select Number Group.**
The Select Line Group page appears.

Step 3 Select a Number group to add to the Hunt Group from the pull-down selection list.

Note The same number group can be added to more than one hunt group.

Step 4 Select the order in which the Number group should be used.

Step 5 Click **Add**.

Number Groups

A Number group is a set of phones that can be used by one or more hunt groups to determine the way that incoming calls are handled when a call is received by the pilot number assigned to the hunt group.

For instructions about creating a number group, see Appendix A, “Location Administration.”

> **Note** Number groups in the location administrator level are called Line Groups.

Pickup Groups

A pickup group is a set of phone numbers that allows a user of any phone in the group to answer an incoming call by pressing a soft key button. Pickup groups are created by customer administrators, but location administrators can add or remove numbers from a pickup group or associate and unassociate pickup groups. When two pickup groups are associated, they function as a single pickup group for as long as they remain associated.

Group pickup allows the user of a phone that is not in the pickup group to also pick up a call. This is achieved by the use of the Group pickup extension number.

This section describes how to add a pickup group to a location. For information about managing pickup groups, including adding lines to the pickup group, see Appendix A, "Location Administration."

To create a pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**. A Pickup Group Management page appears on the screen.
To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add** on the Pickup Group Management page.

Step 3 Enter a unique name for the pickup group.

Step 4 Enter a description for the pickup group (Optional).

Step 5 Select a number that is not within the pick-up group that should pick up a call.

Step 6 Click **Add**.

Users

This section describes how to change permissions for users within a location. For information about creating and managing user accounts, refer to Appendix A, "Location Administration."

To change the permissions for a user, complete the following steps:

Procedure

Step 1 Click **User** on the Location Administration menu.

Step 2 Click the blue link in the Username column for the user account you want to manage, in the User Management page.

Step 3 Click **Permissions**.

Step 4 Click the checkbox to enable or disable the type of permissions the selected user account should have for the operation listed on each line.

Step 5 Click **Modify**.

Phone Inventory

Use the **Phone Inventory** option on the Location Administration menu to manage the phone inventory in the current location.

To manage the phone inventory, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the General Administration Menu.
A Phone Inventory page containing a list of the phone inventory in the current location, is displayed. You can use this page to search for phones in the database and to manage a specific phone.

Step 2 To manage a phone, click the blue link in the Name column.

Step 3 To add a voicemail account, click **Add**.

Step 4 This page displays information about the selected phone.

Phone Registration

Use the **Phone Registration** option on the Location Administration menu to register phones in the current location.

After a phone is assigned to a location it is assigned its IP address and appears in the USM database in the Unregistered state. However, the phone is registered with Unified CM and can be used to make calls to internal extensions and to make emergency calls. When a call is placed to an emergency number from a phone in this state, the dialing number used is the emergency number assigned to the location.

When the phone is registered, it is assigned a feature group and an external (DDI) number. After registration, the phone can be used for logging in to a Mobility profile, and can be used to make calls to external numbers.

To register a phone, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration Menu.
A Phone Registration page containing a list of the unregistered phones in the current location, is displayed. You can use this page to search for unregistered phones in the database, to register a specific phone, unregister a phone, or display phone status.

Step 2 To register a phone, click the blue link in the Name column.

For further information about registering phones, see Appendix A, "Location Administration."

Phone Management

Use the **Phone Management** option on the Location Administration menu to manage the phones within a location. For information about managing phones within a location, see Appendix A, "Location Administration."

Analogue Line Mgt.

Use the **Analogue Line Mgt.** option on the Location Administration menu to register an analog line (for example, for a fax machine) and associate a phone number with the line. To register an analog line, you need the following information:

- Analogue gateway address: for example, 12.34.56.78.AB.90
- Feature group for the Analogue Line
- Telephone number allocated for the line: for example, 86644000

When registering an analog line, note the following:

- You must register an analog line from the Location level.
- The analog gateway must be provisioned for the location.

To register an analog line, complete the following steps:

Procedure

Step 1 Select **Analogue Line Mgt.** on the Location Administration menu.
An Analogue Port Management page containing a list of the analogue ports in the current location, is displayed. You can use this page to search for switchboards in the database, to manage a specific switchboard, or add a switchboard.

Step 2 To manage an existing analogue port, click the blue link in the Name column.

Step 3 On the page that appears, click **Gateway name**.

Step 4 On the page that appears, select the port that you wish to register from the pull-down selection list.

Step 5 Click **Next**.

Step 6 Enter the relevant phone numbers (E.164, DDI, and local extensions).

Step 7 Click **Register**.

MoH Track Mgt Option

Use the Unified CM Administration pages to add music on hold (MoH) tracks to the Hosted UCS system.

Use the **MoH Track Mgt** option on the Location Administration menu to manage MoH tracks.

To manage MoH tracks, complete the following steps:

Procedure

Step 1 Select **MoH Track Mgt** on the Location Administration Menu.
A MoH Track Management page containing a list of the MoH tracks in the current location, is displayed. You can use this page to search for MoH tracks in the database, to manage a specific MoH track, or add a MoH track.

Step 2 To manage an existing MoH track, click the blue link in the Name column.

Step 3 To add a MoH track, click **Add**.

Step 4 Enter the following details:

- MoH Track Name
- Track ID
- Description of Track
- MoH Server Name.

Step 5 Click **Submit**.

The Hosted UCS system adds the MoH Track to the database.

Internal Numbers

DDI numbers must be associated with an internal number before allocation. The service provider. If DDI numbers are not present, or you have used all your numbers, request additional numbers from the service provider.

Range association allows a set of external numbers to be linked together with a range of internal numbers. Number association is required to ensure that all DDI numbers assigned to a phone or Mobility profile always have an internal number for internal calls. It is also possible to bulk load the DDI numbers and range association.

Use the **Internal Numbers** option on the Location Administration menu to manage internal numbers.

To manage internal numbers, complete the following steps:

Procedure

Step 1 Select **Internal Numbers** on the Location Administration Menu.
A Manage available internal numbers page containing a list of internal numbers, their associated PSTN numbers, their associated phone users, switchboard pilot, and type of phone, is displayed. You can use this page to search for internal numbers in the database, or to manage the internal number range.

Note You cannot reserve a number if it has already been associated.

Step 2 To manage the internal number range, click **Internal Number Range Mgt.**

Step 3 Enter the starting range for the internal numbers in the Start Internal Number field.

Step 4 Select the number of internal numbers from the Range Size pull-down selection list.

Step 5 Click one of the following buttons, depending on how you want to manage:

- **Enable**—Enable the selected range of internal numbers.
- **Disable—**Disable the selected range of internal numbers.
- **Reserve—**Reserve the selected range of internal numbers.
- **Unreserve**—Unreserve the selected range of internal numbers.

External Numbers

Use the **External Numbers** option on the Location Administration menu to manage external numbers.

To manage external numbers, complete the following steps:

Procedure

Step 1 Select **External Numbers** on the Location Administration Menu.
A Manage External Numbers Usage page is displayed. The Manage External Numbers usage page allows you to review the association between DDI and Internal numbers for you location, as well as removing the association for certain numbers. To disassociate numbers click **DisAssoc** next to the relevant DDI number. You can use this page to search for external numbers in the database, to disassociate a specific number, to disassociate a range, or to associate a range.

Step 2 To associate a range, click **Range Assoc.**

Step 3 Select the national Code from the pull-down selection list.

Step 4 Select the start of the range, end of range, and extension numbers to associate from the pull-down selection lists.

Step 5 Click **Submit**.

APPENDIX D

Sample PGW, Unified CM, and IP Unity Transactions

Revised: 08/12/2010, OL-23270-01

This document explains the sample PGW, Unified CM and IP Unity transactions in Unified UCS.

Associate IP Unity VoiceMail Server with PGW Transaction

USM invokes the PGW driver and uses the mml scripts in the ConnectTransitToVMSvr transaction (ConnectTransitToVMSvr-IPUnity mml script name) of the PGW model worksheet to configure the EGRV dial plan to detect calls destined for IP Unity, modify the B number, and route the call to IP Unity.

For example

```
;ConnectTransitToVMSvr-IPUnity:
; 032 A CPID for the IP UNITY system.
;EGRV DP - Result set to modified B number to Nat. and route it to IPUNITY
numan-add:resultset:custgrpid="EGRV",name="gotoIpUnity"
numan-add:Resulttable:custgrpid="EGRV",name="setBnoaNat",resulttype="B_NUMBER_TYPE",setnam
e="gotoIpUnity",dw1="4"
numan-add:resulttable:custgrpid="EGRV",name="gotoIpUnity",resulttype="ROUTE",dw1="rtlist2i
punity",setname="gotoIpUnity"
;EGRV DP - B Number Analysis -ResultSet gotoIPUnity trigger on IpUnity CPID
numan-add:bdigtree:custgrpid="EGRV",callside="originating",digitstring="032",setname="goto
IpUnity"
```

Associate Unified CM Cluster with PGW for MWI Support Transaction

USM invokes the PGW driver and uses the mml scripts in the ConnectIPPBXTransit transaction (ConnectIPPBXTransit mml script name) of the PGW model worksheet to configure the ROUT dial plan to detect MWI calls from IP Unity to the customer's phones

For example

```
; ConnectIPPBXTransit: add per-CCM cluster support for MWI signals when Cluster is
connected to PGW that is directly connected to IP Unity
 ; 101 A CPID for the IP PBX system.
; 9999 A constant of All 9's to length of RIDs in the system.
;  Can't used 9999 , change to 9999 A constant of All 9's to length of RIDs in the system.
; Add entry into ROUT to handle MWI calls from IP Unity calls to this customer s phones
numan-add:bdigtree:custgrpid="ROUT",callside="originating",digitstring="1019999",setname="
MWItoHSI"
```

Add Voicemail Service

USM invokes the PGW driver and uses the mml scripts in the ConnectIPPBXTransit transaction (AddVMService-IPUnity mml script name) of the PGW model worksheet to do the following:

- ICCM dial plan to route MWI calls from Movius to correct per-customer vmail dialplan., prefix an A the B number and switch analysis to VOICEMAILDIALPLAN base on the AA service pilot FINT
- Add VM Service into Per-customer Ingress (#CUSTDIALPLAN#, for example 0005) dial plan

- Per-country (R#PADDEDCC#, for example R044) dial plan, PSTN to voicemail calls, prefix B with Movius CPID+RID
- Per Custome Voicemail Dial plan (#VOICEMAILDIALPLAN, i. e. 000G), to support outgoing calls from Movius

For example:

```
; AddVMService-IPUnity: add Customer support for voicemail
; 0005 - Customer DialPlan
; 000G Voicemail Service Dialplan
; 032 A CPID for the IP UNITY system.
; 1001 A RID that uniquely identifies a VM Service
; 9999 A constant of All 9's to length of RIDs in the system.
; 666 Voicemail Service Site Code
; 10 - CPID+RID+SLC DIGITS
; 9 - pstn breakout code for voicemail
; 90 - pstn breakout code plus National Direct Dialing Code
; 2 - EXT plus NDD digits
; 944 - pstn breakout code plus International Direct Dialing Code
; 3 - EXT plus IDD digits
; 8 - intersite prefix
; 100 - CCM Cluster CPID
; 1009999999001 - The MWI On number on the cluster
; 1009999999002 The MWI Off number on the cluster
; 11 - sizeof FINT + 1
; 11 - sizeof FINT + 2
; 3 - sizeof (VMEXTNNDD) + 1
; 4 sizeof (VMEXTNIDD) + 1
;
numan-add:dialplan:custgrpid="000G", OVERDEC="YES"
numan-add:dpsel:custgrpid="ICCM",newdp="000G"
numan-add:dpsel:custgrpid="000G",newdp="ROUT"
;allow change to Cust specific MWI dialplan
numan-add:resultset:custgrpid="ICCM",name="chgdplCust000GMWI"
numan-add:resulttable:custgrpid="ICCM",name="chgdplCust000GMWI",resulttype="NEW_DIALPLAN",
dw1="000G",setname="chgdplCust000GMWI"
; check for per-customer voicemail pilot to route MWI calls from IP unity to correct
per-customer vmail dialplan;
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitstring="0321001",setname="
chgdplCust000GMWI"
; Resultset to prefix A to the B number and switch analysis to VOICEMAILDIALPLAN base on
the AA service pilot FINT (the A number ) from ICCM
numan-add:resultset:custgrpid="ICCM",name="chgdplCust000GAA"
numan-add:resulttable:custgrpid="ICCM",name="chgdplCust000GAA",resulttype="NEW_DIALPLAN",d
w1="000G",setname="chgdplCust000GAA"
numan-add:resulttable:custgrpid="ICCM",name="pfxA2Bnum",resulttype="BMODDIG",dw1="1",dw2="
0",dw3="addA2Bnum",setname="chgdplCust000GAA"
;
; add  VM service routing into customer dialplan
numan-add:digmodstring:custgrpid="0005",name="0321001siteE164",digstring="83CCC6660000"
numan-add:resultset:custgrpid="0005", name="0321001CR9FNT"
numan-add:resulttable:custgrpid="0005",name="acr9fnt",resulttype="NUM_TRANS",
dw1="0005cr9fnt", dw2="2",dw3="5",setname="0321001CR9FNT"
numan-add:resulttable:custgrpid="0005",name="0321001siteE164",resulttype="AMODDIG",dw1="1"
,dw2="99",dw3="0321001siteE164",setname="0321001CR9FNT"
numan-add:adigtree:custgrpid="0005",callside="originating",digitstring="03210019",setname=
"0321001CR9FNT"
;
numan-add:digmodstring:custgrpid="0005",name="CRVM0321001",digstring="0321001"
numan-add:resultset:custgrpid="0005",name="VMSvc0321001"
numan-add:resulttable:custgrpid="0005",name="BVM0321001",resulttype="BMODDIG",dw1="1",dw2=
"1",dw3="CRVM0321001",setname="VMSvc0321001"
```

```
numan-add:resulttable:custgrpid="0005",name="RtVM0321001",resulttype="NEW_DIALPLAN",dw1="R
OUT",dw2="1",setname="VMSvc0321001"
;B handle, call is to onnet vmail pilot, add CR to B for C1 vmail partition. Go to next
dialplan, RDN is already modded by A RDN case
numan-add:bdigtree:custgrpid="0005",callside="originating",digitstring="8666",setname="VMS
vc0321001"
;
;PSTN to voicemail calls, prefix B with IPUnity CPID+RID. Now consistent with routing to
sites.
numan-add:digmodstring:custgrpid="R044",name="C1001VMpilot",digstring="0321001"
numan-add:resultset:custgrpid="R044",name="0321001addCRsite"
numan-add:resulttable:custgrpid="R044",name="C1001addVMCR",resulttype="BMODDIG",dw1="1",dw
2="0",dw3="C1001VMpilot",setname="0321001addCRsite"
numan-add:resulttable:custgrpid="R044",name="gotoROUT",resulttype="NEW_DIALPLAN",dw1="ROUT
",dw2="1",setname="0321001addCRsite"
; Add entry into ROUT to handle calls to IP Unity calls for this customer
numan-add:bdigtree:custgrpid="ROUT",callside="originating",digitstring="0321001",setname="
gotoEGRV"
; Add outdialing support for Voicemail service
numan-add:dpsel:custgrpid="000G",newdp="0005"
numan-add:digmodstring:custgrpid="000G",name="PSTN90",digstring="90"
numan-add:digmodstring:custgrpid="000G",name="PSTN900",digstring="900"
numan-add:digmodstring:custgrpid="000G",name="CallType9",digstring="9"
numan-add:digmodstring:custgrpid="000G",name="Intersite",digstring="8"
; resultset to handle AA transfers to PSTNNAT
numan-add:resultset:custgrpid="000G",name="AATfrPstnNat"
numan-add:resulttable:custgrpid="000G",name="goto0005",resulttype="NEW_DIALPLAN",dw1="0005
",dw2="1",setname="AATfrPstnNat"
numan-add:resulttable:custgrpid="000G",name="Bpref90",resulttype="BMODDIG",dw1="1",dw2="2"
,dw3="PSTN90",setname="AATfrPstnNat"
numan-add:resulttable:custgrpid="000G",name="APSTNAA",resulttype="AMODDIG",dw1="8",dw2="0"
,dw3="CallType9",setname="AATfrPstnNat"
; resultset to handle AA transfers to PSTNINTL
numan-add:resultset:custgrpid="000G",name="AATfrPstnIntl"
numan-add:resulttable:custgrpid="000G",name="goto0005",resulttype="NEW_DIALPLAN",dw1="0005
",dw2="1",setname="AATfrPstnIntl"
numan-add:resulttable:custgrpid="000G",name="Bpref900",resulttype="BMODDIG",dw1="1",dw2="3
",dw3="PSTN900",setname="AATfrPstnIntl"
numan-add:resulttable:custgrpid="000G",name="APSTNAA",resulttype="AMODDIG",dw1="8",dw2="0"
,dw3="CallType9",setname="AATfrPstnIntl"
; resultset to handle AA transfers to Extensions
numan-add:resultset:custgrpid="000G",name="AATfrExtn"
numan-add:resulttable:custgrpid="000G",name="goto0005",resulttype="NEW_DIALPLAN",dw1="0005
",dw2="1",setname="AATfrExtn"
numan-add:resulttable:custgrpid="000G",name="BprefISP",resulttype="AMODDIG",dw1="8",dw2="0
",dw3="Intersite",setname="AATfrExtn"
numan-add:resulttable:custgrpid="000G",name="Bpref90",resulttype="BMODDIG",dw1="1",dw2="1"
,dw3="Intersite",setname="AATfrExtn"
numan-add:resulttable:custgrpid="000G",name="setBnoaInternal",resulttype="B_NUMBER_TYPE",d
w1="48",setname="AATfrExtn"
;CT=8  - OnNet calls -
numan-add:adigtree:custgrpid="0005",callside="originating",digitstring="03210018",setname=
"C1stripCRaddiPX"
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="90",setname="AATfr
PstnNat"
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="944",setname="AATf
rPstnIntl"
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="8",setname="AATfrE
xtn"
;
; B number Analysis to handle AA calls
; InterSite Calls
numan-add:digmodstring:custgrpid="000G",name="addAAtoAnum",digstring="AA"
numan-add:resultset:custgrpid="000G",name="AAInterSiteCall"
```

```
numan-add:resulttable:custgrpid="000G",name="modA",resulttype="AMODDIG",dw1="1",dw2="11",d
w3="addAAtoAnum",setname="AAInterSiteCall"
numan-add:resulttable:custgrpid="000G",name="modB",resulttype="BMODDIG",dw1="1",dw2="2",dw
3="Intersite",setname="AAInterSiteCall"
numan-add:resulttable:custgrpid="000G",name="switch2CustDP",resulttype="NEW_DIALPLAN",dw1=
"0005",dw2="1",setname="AAInterSiteCall"
;
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="A8",setname="AAInt
erSiteCall"
;
; National Calls
numan-add:resultset:custgrpid="000G",name="AANatlCall"
numan-add:resulttable:custgrpid="000G",name="modA",resulttype="AMODDIG",dw1="11",dw2="99",
setname="AANatlCall"
numan-add:resulttable:custgrpid="000G",name="modB",resulttype="BMODDIG",dw1="1",dw2="3",dw
3="PSTN90",setname="AANatlCall"
numan-add:resulttable:custgrpid="000G",name="switch2CustDP",resulttype="NEW_DIALPLAN",dw1=
"0005",dw2="1",setname="AANatlCall"
;
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="A90",setname="AANa
tlCall"
;
; International Calls
numan-add:resultset:custgrpid="000G",name="AAIntlCall"
numan-add:resulttable:custgrpid="000G",name="modA",resulttype="AMODDIG",dw1="11",dw2="99",
setname="AAIntlCall"
numan-add:resulttable:custgrpid="000G",name="modB",resulttype="BMODDIG",dw1="1",dw2="4",dw
3="PSTN900",setname="AAIntlCall"
numan-add:resulttable:custgrpid="000G",name="switch2CustDP",resulttype="NEW_DIALPLAN",dw1=
"0005",dw2="1",setname="AAIntlCall"
;
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="A944",setname="AAI
ntlCall"
;
;MWI  handling for customer - change to the customer's MWI dialplan
```

Add VoiceMail Pilot Number Transaction on PGW

USM invokes the PGW driver and uses the mml scripts in the AddVMServicePilot transaction (AddVMServicePilotIPPBX-IPUnity mml script name) of the PGW model worksheet to configure the per-customer VoiceMail Dial Plan MWI On and Off Numbers. This is done per each CUCM cluster associated on 2.3.6

For example

```
;AddVMServicePilotIPPBX-IPUnity:  add logic for connecting CCM cluster to voicemail when
CCM is connected to PGW with direct connection to IP Unity
; 000G A unique dialplan number within PGW to be used for the customer s
voicemailintegration.
; 100 This is the CPID of the CCM cluster. This value changes each time the routine is
called.
; 9999 All 9's to length of RIDs in the system.
; 666 All 9's to length of Site Location Codes in the system.
; 001 Constant Digit string used within the "MWI On" number. The MWI On number on each
cluster will be 1009999666001
; 002 Constant Digit string used within the "MWI Off" number. The MWI Off number on each
cluster will be 1009999666002
;
;MWI  handling for customer - change to the customer's MWI dialplan
numan-add:digmodstring:custgrpid="000G",name="Cluster100MWIon",digstring="1009999666001"
```

```
numan-add:digmodstring:custgrpid="000G",name="Cluster100MWIoff",digstring="1009999666002"
```

Add VoiceMail Pilot Number Transaction on Movius

USM invokes the “IP Unity Any” driver and uses the XML scripts in the AddVMServicePilot transaction (Movius_xml table name) of the IPUnity model worksheet to create and configure a per-customer Organization.

For example:


```
<AddOrgRequest requestId="">
<IAOrganization>
<General>
<name>e3VMSCust1</name>
<callerEmailId>caller@E3Cust1.com</callerEmailId>
<Telephone>
<phoneType>1</phoneType>
<telephone>0321001666099</telephone>
<countryCode>44</countryCode>
</Telephone>
<isResidentialOrg>false</isResidentialOrg>
<autoAttEnabled>false</autoAttEnabled>
<timeZoneId>13</timeZoneId>
<storeVoiceFaxInSeparateFolder>false</storeVoiceFaxInSeparateFolder>
<unheardMsgQEnabled>false</unheardMsgQEnabled>
<defaultTutorialId>0</defaultTutorialId>
<webPasswordPolicyName>default_email</webPasswordPolicyName>
<tuiPasswordPolicyName>default_tui</tuiPasswordPolicyName>
<scheduleBasedAAMenusEnabled>false</scheduleBasedAAMenusEnabled>
<centrixId>8</centrixId>
</General>
<EmailSpecific>
<domain>E3Cust1.com</domain>
<mailServerId>101</mailServerId>
<unifiedMessagingEnabled>false</unifiedMessagingEnabled>
<integratedMessagingEnabled>false</integratedMessagingEnabled>
</EmailSpecific>
<FaxSpecific>
<faxEnabled>false</faxEnabled>
<outboundFaxServerId>0</outboundFaxServerId>
</FaxSpecific>
<Quota>
<maxNumberOfUser>9</maxNumberOfUser>
<maxVoiceMailSize>1000</maxVoiceMailSize>
<quotaWarningLevel>80</quotaWarningLevel>
<quotaMsgSendInterval>12</quotaMsgSendInterval>
</Quota>
<OutCall>
<callSenderEnabled>false</callSenderEnabled>
<placeACallEnabled>false</placeACallEnabled>
<numberingPlanID>101</numberingPlanID>
<mwiCAID>101</mwiCAID>
<outgoingCAID>101</outgoingCAID>
<mwiCallAgentType>1</mwiCallAgentType>
</OutCall>
<MessageWaitingNotification>
<mwnByPhoneEnabled>true</mwnByPhoneEnabled>
<mwnByNumericPageEnabled>true</mwnByNumericPageEnabled>
<mwnByTextPageEnabled>true</mwnByTextPageEnabled>
</MessageWaitingNotification>
```

```
<OrganizationAdmin>
<emailId>admin1</emailId>
<emailPassword>PASSWORD:1</emailPassword>
<adminMB>9888</adminMB>
<password>45123</password>
</OrganizationAdmin>
<Miscellaneous>
<firstNameLastName>false</firstNameLastName>
<defMWStartHour>9</defMWStartHour>
<defMWStopHour>17</defMWStopHour>
<defMWRetryPer>30</defMWRetryPer>
<defNumPageString>1111</defNumPageString>
<outcallSpkTimes>3</outcallSpkTimes>
<defMsgMaxRcrdTime>5</defMsgMaxRcrdTime>
<maxFwdDepth>5</maxFwdDepth>
<playSenderNameEnabled>true</playSenderNameEnabled>
<revwPlayTimestampEnabled>true</revwPlayTimestampEnabled>
<rcvMsgEAGEnabled>true</rcvMsgEAGEnabled>
<msgScanVoiceMailEnabled>true</msgScanVoiceMailEnabled>
<autoPlayVoiceMails>true</autoPlayVoiceMails>
<msgScanAllMailsEnbaled>true</msgScanAllMailsEnbaled>
<autoPlayAllMailsEnabled>true</autoPlayAllMailsEnabled>
<autoSkipNextMsgEnabled>true</autoSkipNextMsgEnabled>
<fwdPrivateMsgEnabled>true</fwdPrivateMsgEnabled>
<firstLoginChngPasswdEnabled>true</firstLoginChngPasswdEnabled>
<firstLoginRcrdNameEnabled>true</firstLoginRcrdNameEnabled>
<firstLoginRcrdGtgEnabled>true</firstLoginRcrdGtgEnabled>
<rootPathId>101</rootPathId>
</Miscellaneous>
<subscriberMessagingControl>
<sendMsgBlocked>true</sendMsgBlocked>
<sendMsgNetworkAddressBlocked>true</sendMsgNetworkAddressBlocked>
<sendMsgOdlBlocked>false</sendMsgOdlBlocked>
</subscriberMessagingControl>
<MessageDeliveryToPhoneNumber>
<messageDeliveryToPhoneNumberEnabled>true</messageDeliveryToPhoneNumberEnabled>
<checkDtmfForMsgPlayEnabled>false</checkDtmfForMsgPlayEnabled>
<defaultMsgPlayWaitTime>5</defaultMsgPlayWaitTime>
</MessageDeliveryToPhoneNumber>
<callTransferSettingsForOutsideCaller>
<transferLocalLongBlocked>true</transferLocalLongBlocked>
<transferDomesticLongBlocked>false</transferDomesticLongBlocked>
<transferInternationalBlocked>true</transferInternationalBlocked>
</callTransferSettingsForOutsideCaller>
<networkMessaging>
<networkAddressingAllowed>true</networkAddressingAllowed>
<useSystemNetworkAddresses>true</useSystemNetworkAddresses>
</networkMessaging>
</IAOrganization>
</AddOrgRequest>
```


Associate E164 Number to VoiceMail Pilot Number Transaction

USM invokes the PGW driver and adds 3 lines to the FNT x10 DB table to do the following:

- Per-customer Ingress (#CUSTDIALPLAN#, for example 0005) dial plan, to detect and convert the configured VoiceMail Pilot number to E164 number
- Per-customer Egress (#EGRESSCUSTDIALPLAN#, for example 0006) dial plan, to detect and convert the configured E164 number to VoiceMail Pilot number

- Per-country (R#PADDEDCC#, for example R044) dial plan, to detect the configured E164 number.

For example:

```
FNT,0005cr9fnt,2,03210019666099,E441640666099
FNT,0006afnt,2,441640666099,E666099
FNT,r044bfnt,1,441640666099,0321001666099
```

back to Associating E164 Number to VoiceMail Pilot Number (Section 2.4.5)

Add Location VoiceMail Service Transaction on PGW

USM invokes the PGW driver and uses the mml scripts in the AddLocationVM transaction (AddLocationVM-IPUnity mml script name) of the PGW model worksheet to configure the per-customer VoiceMail dial plan (for example 000G) with per-location logic to support MWI calls from IP Unity.

For example:

```
; AddLocationVM-IPUnity: add per location logic to support Mwi calls from IP unity.
; 000G A unique dialplan number within PGW to be used for the customer s voicemail
integration
; 100 CPID for the CCM Cluster where the location resides.
; 0010 RID for the new location.
; 111 The Site Location Code (SLC) for the new location
;-----------------------------------------------------------------------------------
numan-add:digmodstring:custgrpid="000G",name="MWI1000010",digstring="1000010"
numan-add:resultset:custgrpid="000G",name="CR1000010"
numan-add:resulttable:custgrpid="000G",name="prefCR1000010",resulttype="BMODDIG",dw1="1",d
w2="0",dw3="MWI1000010",setname="CR1000010"
numan-add:resulttable:custgrpid="000G",name="MWIflip",resulttype="B_NBR_MOD_MWI",dw1="Clus
ter100MWIon",dw2="Cluster100MWIoff",setname="CR1000010"
numan-add:resulttable:custgrpid="000G",name="gotoROUT",resulttype="NEW_DIALPLAN",dw1="ROUT
",dw2="1",setname="CR1000010"
; if the B-number from IP Unity starts with the location s Site Location Code then use the
result-set created above
numan-add:bdigtree:custgrpid="000G",callside="originating",digitstring="111",setname="CR10
00010"
```

Add Location VoiceMail Service Transaction on Unified CM

USM invokes the IPPBX driver on the selected Unified CM Cluster to do the following:

- Remove Route Pattern, page D-9
- Add Route Pattern, page D-9
- Remove Route Pattern, page D-9
- Add Route Pattern, page D-10
- Remove Translation Pattern, page D-10
- Add Translation Pattern, page D-11
- Add Voicemail Pilot, page D-11
- Add Voicemail Profile, page D-11

- Update all phones in the location, page D-12
- Update all lines in the phone with the VM Profile, page D-13
- Remove Translation pattern, CSS and partition for PLAR, page D-14

Remove Route Pattern


```
<removeRoutePattern xmlns="http://10.134.3.2/">
<pattern>8.666!</pattern>
<routePartitionName>AllowVMCalls10</routePartitionName>
<routeFilterName>
</routeFilterName>
</removeRoutePattern>
```


Add Route Pattern


```
<newPattern>
<pattern>8.666!</pattern>
<description>AllowVMCalls10</description>
<usage>Device</usage>
<routePartitionName>AllowVMCalls10</routePartitionName>
<blockEnable>false</blockEnable>
<calledPartyTransformationMask>
</calledPartyTransformationMask>
<callingPartyTransformationMask>10000108111XXX</callingPartyTransformationMask>
<useCallingPartyPhoneMask>Off</useCallingPartyPhoneMask>
<callingPartyPrefixDigits>
</callingPartyPrefixDigits>
<dialPlanWizardGenId>
</dialPlanWizardGenId>
<digitDiscardInstructionName>
</digitDiscardInstructionName>
<messageWaiting>Wink</messageWaiting>
<networkLocation>OnNet</networkLocation>
<patternUrgency>false</patternUrgency>
<prefixDigitsOut>
</prefixDigitsOut>
<routeFilterName>
</routeFilterName>
<callingLinePresentationBit>Default</callingLinePresentationBit>
<callingNamePresentationBit>Allowed</callingNamePresentationBit>
<releaseCause>Call Rejected</releaseCause>
<provideOutsideDialtone>false</provideOutsideDialtone>
<destination>
<routeListName>VOICEMAIL</routeListName>
<provideOutsideDialtone>false</provideOutsideDialtone>
</destination>
<clientCodeRequired>false</clientCodeRequired>
</newPattern>
</addRoutePattern>
```


Remove Route Pattern


```
<removeRoutePattern xmlns="http://10.134.3.2/">
<pattern>8.666!</pattern>
```

```
&lt;routePartitionName&gt;AllowVMCallsCF10&lt;/routePartitionName&gt;
&lt;routeFilterName&gt;
&lt;/routeFilterName&gt;
&lt;/removeRoutePattern&gt;
```

Add Route Pattern

```
&lt;addRoutePattern xmlns="http://10.134.3.2/"&gt;
&lt;newPattern&gt;
&lt;pattern&gt;8.666!&lt;/pattern&gt;
&lt;description&gt;AllowVMCallsCF10&lt;/description&gt;
&lt;usage&gt;Device&lt;/usage&gt;
&lt;routePartitionName&gt;AllowVMCallsCF10&lt;/routePartitionName&gt;
&lt;blockEnable&gt;false&lt;/blockEnable&gt;
&lt;calledPartyTransformationMask&gt;
&lt;/calledPartyTransformationMask&gt;
&lt;callingPartyTransformationMask&gt;
&lt;/callingPartyTransformationMask&gt;
&lt;useCallingPartyPhoneMask&gt;Off&lt;/useCallingPartyPhoneMask&gt;
&lt;callingPartyPrefixDigits&gt;10000106&lt;/callingPartyPrefixDigits&gt;
&lt;dialPlanWizardGenId&gt;
&lt;/dialPlanWizardGenId&gt;
&lt;digitDiscardInstructionName&gt;
&lt;/digitDiscardInstructionName&gt;
&lt;messageWaiting&gt;Wink&lt;/messageWaiting&gt;
&lt;networkLocation&gt;OnNet&lt;/networkLocation&gt;
&lt;patternUrgency&gt;false&lt;/patternUrgency&gt;
&lt;prefixDigitsOut&gt;
&lt;/prefixDigitsOut&gt;
&lt;routeFilterName&gt;
&lt;/routeFilterName&gt;
&lt;callingLinePresentationBit&gt;Default&lt;/callingLinePresentationBit&gt;
&lt;callingNamePresentationBit&gt;Allowed&lt;/callingNamePresentationBit&gt;
&lt;releaseCause&gt;Call Rejected&lt;/releaseCause&gt;
&lt;provideOutsideDialtone&gt;false&lt;/provideOutsideDialtone&gt;
&lt;destination&gt;
&lt;routeListName&gt;VOICEMAIL&lt;/routeListName&gt;
&lt;provideOutsideDialtone&gt;false&lt;/provideOutsideDialtone&gt;
&lt;/destination&gt;
&lt;clientCodeRequired&gt;false&lt;/clientCodeRequired&gt;
&lt;/newPattern&gt;
&lt;/addRoutePattern&gt;
```

Remove Translation Pattern

```
&lt;removeTransPattern xmlns="http://10.134.3.2/"&gt;
&lt;pattern&gt;#1#.1000010!&lt;/pattern&gt;
&lt;routePartitionName&gt;IncomingFromIPU&lt;/routePartitionName&gt;
&lt;routeFilterName&gt;
&lt;/routeFilterName&gt;
&lt;/removeTransPattern&gt;
```

Add Translation Pattern

```
<addTransPattern xmlns="http://10.134.3.2/">
<newPattern>
<pattern>#1#.1000010!</pattern>
<description>Voicemail</description>
<usage>Device</usage>
<routePartitionName>IncomingFromIPU</routePartitionName>
<blockEnable>false</blockEnable>
<calledPartyTransformationMask>
</calledPartyTransformationMask>
<callingPartyTransformationMask>
</callingPartyTransformationMask>
<useCallingPartyPhoneMask>Off</useCallingPartyPhoneMask>
<callingPartyPrefixDigits>
</callingPartyPrefixDigits>
<dialPlanWizardGenId>
</dialPlanWizardGenId>
<digitDiscardInstructionName>Predot</digitDiscardInstructionName>
<messageWaiting>Wink</messageWaiting>
<networkLocation>OnNet</networkLocation>
<patternUrgency>true</patternUrgency>
<prefixDigitsOut>
</prefixDigitsOut>
<routeFilterName>
</routeFilterName>
<callingLinePresentationBit>Default</callingLinePresentationBit>
<callingNamePresentationBit>Default</callingNamePresentationBit>
<provideOutsideDialtone>false</provideOutsideDialtone>
<callingSearchSpaceName>IncomingToCluster</callingSearchSpaceName>
</newPattern>
</addTransPattern>
```

Add Voicemail Pilot

```
<addVoiceMailPilot xmlns="http://10.134.3.2/">
<voiceMailPilot>
<dirn>8666099</dirn>
<description>VM Pilot for location10</description>
<CSSName>Voicemail10</CSSName>
<isDefault>false</isDefault>
</voiceMailPilot>
</addVoiceMailPilot>
```

Add Voicemail Profile

```
<addVoiceMailProfile xmlns="http://10.134.3.2/">
<voiceMailProfile>
<name>VMProfile110</name>
<description>VM Profile for location10</description>
<isDefault>false</isDefault>
<voiceMailPilot uuid="{C713DD9C-8B49-3692-B12D-42BFFD7DA116}">
</voiceMailPilot>
</voiceMailProfile>
</addVoiceMailProfile>
```

Update all phones in the location

For example

```
<updatePhone xmlns="http://10.134.3.2/">
<name>SEP001DA21A1E52</name>
<callingSearchSpaceName>EmergencyOnly10</callingSearchSpaceName>
<devicePoolName>devicepool10</devicePoolName>
<locationName>location-bvsm-10</locationName>
<networkHoldMOHAudioSourceId>0</networkHoldMOHAudioSourceId>
<userHoldMOHAudioSourceId>0</userHoldMOHAudioSourceId>
<aarNeighborhoodName>
</aarNeighborhoodName>
<vendorConfig>
<disableSpeaker>false</disableSpeaker>
<disableSpeakerAndHeadset>false</disableSpeakerAndHeadset>
<forwardingDelay>1</forwardingDelay>
<pcPort>0</pcPort>
<settingsAccess>1</settingsAccess>
<garp>1</garp>
<voiceVlanAccess>1</voiceVlanAccess>
<videoCapability>0</videoCapability>
<autoSelectLineEnable>0</autoSelectLineEnable>
<webAccess>0</webAccess>
</vendorConfig>
<lines>
<line uuid="{cff950f0-6380-b958-60f4-3161d4779bbe}" index="1">
<label>005</label>
<display>
</display>
<dirn uuid="{cff950f0-6380-b958-60f4-3161d4779bbe}">
</dirn>
<ringSetting>Use System Default</ringSetting>
<consecutiveRingSetting>Use System Default</consecutiveRingSetting>
<e164Mask>1640111005</e164Mask>
<maxNumCalls>4</maxNumCalls>
<busyTrigger>2</busyTrigger>
<mwlPolicy>Use System Policy</mwlPolicy>
</line>
</lines>
<phoneTemplateName>Standard 7945 SIP</phoneTemplateName>
<speeddials>
</speeddials>
<busyLampFields>
</busyLampFields>
<blfDirectedCallParks>
</blfDirectedCallParks>
<userLocale>English United States</userLocale>
<networkLocale>United Kingdom</networkLocale>
<deviceSecurityMode>Use System Default</deviceSecurityMode>
<idleTimeout>
</idleTimeout>
<idleURL>
</idleURL>
<services>
<service uuid="{73a4d252-cc52-8db9-4802-c86a8deed384}">
<telecasterServiceName>Login/Logout</telecasterServiceName>
<name>Login/Logout</name>
<url>http://10.134.3.2:8080/emapp/EMAppServlet?device=#DEVICENAME#</url>
<urlButtonIndex>0</urlButtonIndex>
<urlLabel>Login/Logout</urlLabel>
</service>
```

```
<service uuid="{9cb76602-3a87-25ab-6faa-388b28260dc0}">
<telecasterServiceName>Phone Services</telecasterServiceName>
<name>Phone Services</name>
<url>http://10.100.92.33/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#</url>
<urlButtonIndex>0</urlButtonIndex>
<urlLabel>Phone Services</urlLabel>
</service>
</services>
<softkeyTemplateName>Softkey_Advanced</softkeyTemplateName>
<enableExtensionMobility>true</enableExtensionMobility>
<builtInBridgeStatus>Off</builtInBridgeStatus>
<callInfoPrivacyStatus>Off</callInfoPrivacyStatus>
<ignorePresentationIndicators>false</ignorePresentationIndicators>
<packetCaptureMode>None</packetCaptureMode>
<packetCaptureDuration>0</packetCaptureDuration>
</updatePhone>
```

Update all lines in the phone with the VM Profile

For example

```
<updateLine xmlns="http://10.134.3.2/">
<uuid>{26597e23-b827-985c-45e0-481bac45de84}</uuid>
<newPattern>1000010111001</newPattern>
<description> Line 1000010111001 for a phone</description>
<newRoutePartitionName>Site10</newRoutePartitionName>
<callForwardAll>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<secondaryCallingSearchSpaceName>
</secondaryCallingSearchSpaceName>
<destination>
</destination>
</callForwardAll>
<callForwardBusy>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
</callForwardBusy>
<callForwardBusyInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
</callForwardBusyInt>
<callForwardNoAnswer>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
<duration>12</duration>
</callForwardNoAnswer>
<callForwardNoAnswerInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
<duration>12</duration>
</callForwardNoAnswerInt>
<callForwardNoCoverage>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
<duration>12</duration>
</callForwardNoCoverage>
```

```
<callForwardNoCoverageInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>
</destination>
<duration>12</duration>
</callForwardNoCoverageInt>
<autoAnswer>Auto Answer Off</autoAnswer>
<networkHoldMOHAudioSourceId>0</networkHoldMOHAudioSourceId>
<userHoldMOHAudioSourceId>0</userHoldMOHAudioSourceId>
<alertingName>001</alertingName>
<shareLineAppearanceCSSName>COS1International24Hour10</shareLineAppearanceCSSName>
<voiceMailProfileName>VMProfile110</voiceMailProfileName>
<hrDuration>
</hrDuration>
<hrInterval>
</hrInterval>
<cfaCSSPolicy>With Configured CSS</cfaCSSPolicy>
</updateLine>
```

Remove Translation pattern, CSS and partition for PLAR

```
<removeTransPattern xmlns="http://10.134.3.2/">
<pattern>
</pattern>
<routePartitionName>PLAR1000010111001</routePartitionName>
<routeFilterName>
</routeFilterName>
</removeTransPattern>

<removeCSS xmlns="http://10.134.3.2/">
<name>PLAR1000010111001</name>
</removeCSS>


removeRoutePartition xmlns="http://10.134.3.2/">
<partitionName>PLAR1000010111001</partitionName>
</removeRoutePartition>
```

Add VoiceMail Account Transaction on Unified CM

USM invokes the IPPBX driver on the selected Unified CM Cluster to update the line configured for the user.

For example

```
<updateLine xmlns="http://10.134.3.2/">
<uuid>{29cb4c91-c1c0-0490-666f-4ea4afaf6584}</uuid>
<newPattern>1000010111007</newPattern>
<description> Line 1000010111007 for a phone</description>
<newRoutePartitionName>Site10</newRoutePartitionName>
<callForwardAll>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<secondaryCallingSearchSpaceName>
</secondaryCallingSearchSpaceName>
<destination>
</destination>
</callForwardAll>
```

```
<callForwardBusy>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
</callForwardBusy>
<callForwardBusyInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
</callForwardBusyInt>
<callForwardNoAnswer>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
<duration>12</duration>
</callForwardNoAnswer>
<callForwardNoAnswerInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
<duration>12</duration>
</callForwardNoAnswerInt>
<callForwardNoCoverage>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
<duration>12</duration>
</callForwardNoCoverage>
<callForwardNoCoverageInt>
<callingSearchSpaceName>PSTNIntMobCF10</callingSearchSpaceName>
<destination>8666099</destination>
<duration>12</duration>
</callForwardNoCoverageInt>
<autoAnswer>Auto Answer Off</autoAnswer>
<networkHoldMOHAudioSourceId>
</networkHoldMOHAudioSourceId>
<userHoldMOHAudioSourceId>
</userHoldMOHAudioSourceId>
<alertingName>007</alertingName>
<shareLineAppearanceCSSName>COS1International24Hour10</shareLineAppearanceCSSName>
<voiceMailProfileName>VMProfile110</voiceMailProfileName>
<hrDuration>
</hrDuration>
<hrInterval>
</hrInterval>
<cfaCSSPolicy>With Configured CSS</cfaCSSPolicy>
</updateLine>
```

Add Default VoiceMail Class of Service Transaction

USM invokes the "IP Unity Any" driver and uses the XML scripts in the BasicVoiceMail transaction (IPUnity_model_xml table name) of the IPUnity_Any model worksheet to create and configure the per-organization Class of Service: StandardVoiceMail

For example

```
<AddCosRequest requestId="">
<IACos>
<General>
<orgId>614</orgId>
<name>StandardVoiceMail</name>
<orgProfileID>3</orgProfileID>
<forceRcrdPerGtg>true</forceRcrdPerGtg>
<forceRcrdName>true</forceRcrdName>
```

```
&lt;/General&gt;
&lt;VoiceMail&gt;
&lt;maxNumVoicemails&gt;50&lt;/maxNumVoicemails&gt;
&lt;voiceMsgPurgeTime&gt;14&lt;/voiceMsgPurgeTime&gt;
&lt;replyToOtherAddrsEnabled&gt;true&lt;/replyToOtherAddrsEnabled&gt;
&lt;reqRtrnReceiptEnabled&gt;true&lt;/reqRtrnReceiptEnabled&gt;
&lt;hasInterceptMB&gt;false&lt;/hasInterceptMB&gt;
&lt;msgScanAllMails&gt;true&lt;/msgScanAllMails&gt;
&lt;autoPlayAllMails&gt;true&lt;/autoPlayAllMails&gt;
&lt;scanVoiceMailMessageHeaders&gt;true&lt;/scanVoiceMailMessageHeaders&gt;
&lt;autoSkipNextMsg&gt;true&lt;/autoSkipNextMsg&gt;
&lt;autoPlayVoiceMsgEnabled&gt;true&lt;/autoPlayVoiceMsgEnabled&gt;
&lt;maxVoiceMailSize&gt;5120&lt;/maxVoiceMailSize&gt;
&lt;quotaWarningLevel&gt;80&lt;/quotaWarningLevel&gt;
&lt;maxFDAllowed&gt;5&lt;/maxFDAllowed&gt;
&lt;maxRecordingLength&gt;3&lt;/maxRecordingLength&gt;
&lt;expiryMsgGracePeriodInDays&gt;14&lt;/expiryMsgGracePeriodInDays&gt;
&lt;savedMsgExpiryInDays&gt;7&lt;/savedMsgExpiryInDays&gt;
&lt;allowedToSaveExpiredMessages&gt;true&lt;/allowedToSaveExpiredMessages&gt;
&lt;userConfigPAEnabled&gt;false&lt;/userConfigPAEnabled&gt;
&lt;/VoiceMail&gt;
&lt;Greetings&gt;
&lt;maxNumOfGreetingFiles&gt;2&lt;/maxNumOfGreetingFiles&gt;
&lt;intPGEnabled&gt;false&lt;/intPGEnabled&gt;
&lt;afterHoursGreetingEnabled&gt;false&lt;/afterHoursGreetingEnabled&gt;
&lt;intEAGEnabled&gt;false&lt;/intEAGEnabled&gt;
&lt;enableEAG&gt;true&lt;/enableEAG&gt;
&lt;busyGreetingAllowed&gt;false&lt;/busyGreetingAllowed&gt;
&lt;/Greetings&gt;
&lt;MWI&gt;
&lt;mwiEnabled&gt;true&lt;/mwiEnabled&gt;
&lt;/MWI&gt;
&lt;MWN&gt;
&lt;mwnPhoneEnabled&gt;false&lt;/mwnPhoneEnabled&gt;
&lt;mwnNumPageEnabled&gt;false&lt;/mwnNumPageEnabled&gt;
&lt;mwnTextPageEnabled&gt;false&lt;/mwnTextPageEnabled&gt;
&lt;allowLocalLongDistMWN&gt;false&lt;/allowLocalLongDistMWN&gt;
&lt;allowDomesticDistMWN&gt;false&lt;/allowDomesticDistMWN&gt;
&lt;allowInterDistMWN&gt;false&lt;/allowInterDistMWN&gt;
&lt;/MWN&gt;
&lt;OutCall&gt;
&lt;allowLocalLongDistOutcall&gt;false&lt;/allowLocalLongDistOutcall&gt;
&lt;allowDomesticDistOutcall&gt;false&lt;/allowDomesticDistOutcall&gt;
&lt;allowInterDistOutcall&gt;false&lt;/allowInterDistOutcall&gt;
&lt;allowCallSender&gt;false&lt;/allowCallSender&gt;
&lt;allowPlaceACall&gt;false&lt;/allowPlaceACall&gt;
&lt;/OutCall&gt;
&lt;Email&gt;
&lt;unifiedMessagingEnabled&gt;false&lt;/unifiedMessagingEnabled&gt;
&lt;integratedMessagingEnabled&gt;false&lt;/integratedMessagingEnabled&gt;
&lt;emailQuota&gt;5&lt;/emailQuota&gt;
&lt;/Email&gt;
&lt;Fax&gt;
&lt;faxEnabled&gt;false&lt;/faxEnabled&gt;
&lt;maxFaxPages&gt;20&lt;/maxFaxPages&gt;
&lt;/Fax&gt;
&lt;PDLs&gt;
&lt;maxNumOfPDLs&gt;5&lt;/maxNumOfPDLs&gt;
&lt;maxNumOfMembersPerPDL&gt;10&lt;/maxNumOfMembersPerPDL&gt;
&lt;/PDLs&gt;
&lt;/IACos&gt;
&lt;/AddCosRequest&gt;
```

Add VoiceMail Account Transaction on IP Unity

USM invokes the "IP Unity Any" driver and uses the XML scripts in the AddVoiceMailAcct transaction (IPUnity_model_xml table name) of the IPUnity_Any model worksheet to create and configure a User.

For example

```
<AddUserRequest requestId="2" ver="1">
<orgPilotPhNumber>0321001666099</orgPilotPhNumber>
<mailBoxNum>111007</mailBoxNum>
<IAUser>
<cosProfileId>3</cosProfileId>
<userType>StdMailbox</userType> <firstName>a</firstName>
<lastName>d</lastName>
<emailId>ad</emailId>
<emailPassword>PASSWORD:1</emailPassword>
<password>123456</password>
<outgoingCAID>0</outgoingCAID> <numberingPlanID>101</numberingPlanID>
<telephoneList>
<telephone>
<phoneType>1</phoneType> <telephone>111007</telephone>
<mwiAgentID>0</mwiAgentID>
<language>
<languageID>1</languageID> <langSelectionMenuEnabled>false</langSelectionMenuEnabled>
</language>
</telephone>
</telephoneList>
<mailboxOptions>
<timeZoneId>13</timeZoneId>
<playTimeStampInEnv>true</playTimeStampInEnv>
<playSenderInEnv>false</playSenderInEnv>
<playOldestFirst>false</playOldestFirst>
</mailboxOptions>
<mailFilters>
<ssrVacationEnabled>false</ssrVacationEnabled>
<ssrVacationMessage>xxxxx</ssrVacationMessage>
<ssrRedirectEnabled>false</ssrRedirectEnabled>
<ssrRedirectKeepCopy>false</ssrRedirectKeepCopy>
<ssrRedirectDonotForwardAutomatedMessages>false</ssrRedirectDonotForwardAutomatedMessages>
<ssrRedirectMirror>false</ssrRedirectMirror>
<ssrRedirectForwardTo>a@b.com,c@d.com</ssrRedirectForwardTo>
</mailFilters>
</IAUser>
</AddUserRequest>
```

Adding a AA Pilot on PGW

USM invokes the PGW driver and uses the mml scripts in the AddAAServicePilot transaction (AddAAServicePilot mml script name) of the PGW model worksheet to do the following:

- Configures EGRV dialplan to detect calls to AA and route them to OGAA dial plan
- Configure the per-customer OGAA dial plan to handle calls to AA.
- Configure ICCM to handle calls from AA.

```
; AddAAServicePilot: add Customer support for AutoAttendant
; 0005 - Customer DialPlan
; 000V Voicemail Service Dialplan
; 032 A CPID for the IP UNITY system.
```

```
; 1004 A RID that uniquely identifies a VM Service
; #IPUNITYRESRID# A constant of All 9's to length of RIDs in the system.
; 999 AA Service Site Code
; 098 AA Extension
; EGRV - B number is AA service pilot goto OGAA dp
numan-add:bdigtree:custgrpid="EGRV",callside="originating",digitstring="0321004999098",set
name="switch2OGAA"
; OGAA - Handling call to AA
numan-add:digmodstring:custgrpid="OGAA",name="03210049999098",digstring="03210049999098"
numan-add:resultset:custgrpid="OGAA",name="0321004999098"
numan-add:resulttable:custgrpid="OGAA",name="ApfxFINT",resulttype="AMODDIG",dw1="1",dw2="0
",dw3="03210049999098",setname="0321004999098"
numan-add:resulttable:custgrpid="OGAA",name="gotoIpUnity",resulttype="ROUTE",dw1="rtlist2i
punity",setname="0321004999098"
;
numan-add:bdigtree:custgrpid="OGAA",callside="originating",digitstring="0321004999098",set
name="0321004999098"
;
; Handling call from AA
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitstring="03210049999098",se
tname="chgdplCust000VAA"
```

Enabling Auto Attendant on Movius Organization

USM invokes the "IP Unity Any" driver to enable autoAttendant on the organization:

For example

```
<ModifyOrgRequest requestId="">
<orgId>834</orgId>
<IAOrganization>
<General>
<autoAttEnabled>true</autoAttEnabled>
</General>
</IAOrganization>
</ModifyOrgRequest>
```

Load PGW Transaction

USM invokes the PGW driver and uses the mml scripts in the InitTransit transaction of the PGW MML model worksheet to prepare the initial core dial plans on the PGW:

- CTRY dial plan
- EGRV dial plan
- LOGW dial plan
- ROUT dial plan
- OGAA dial plan
- RDNI dial plan
- RDNO dial plan
- OGAA dial plan

Load Unified CM Clusters Transaction

USM invokes CCM 7.1.x driver and uses the definitions in the InitIPPBX transaction of the CCM model worksheet.

Procedure:

Step 1 Verify that the MOH_<winshostname>; for example, **MOH_e2c1p** is configured on the Unified CM, if the MOH server was selected.

Step 2 Verify that the Login/Logout and Phone Services IP Phone services are configured on the Unified CM.

Step 3 Verify that all phone button templates defined in USM are configured on Unified CM.

Step 4 Verify that the defaultaar has been configured in Unified CMs 5.x, 6.x and 7.x.

Step 5 Create the Unified CM Groups that were defined in USM, for example: **e2PhoneGroupClu1** and **e2TrunkGroupClu1.**

Step 6 Update various Service Parameters. To check which service parameters are updated in USM, do the following:

- **a.** Go to **Network > PBX Devices.**
- **b.** Select the Unified CM clster you want to check the parameters
- **c.** Click View CCM Config
- **d.** Click CCM Cluster Config

Step 7 Create user **ac** (Used for Attendant Console)

Step 8 Create the Time Periods defined in the model: **AllDayEveryDay, StandardBusinessHrs, ExtendedBusinessHrs and WeekendHrs**

Step 9 Create the Time Schedules defined in the model: **alldayeveryday, standardbusinessschedule, extendedbusinessschedule and weekendschedule**

Step 10 Create non-site specific Partitions: **IncominToCluster**, **IncomingFromIPU, IncomingFromOffnet, OutOfService, NullPartition, and AllowMWI**

Step 11 Create Non-Site specific CSSs: **IncomingToCluster, IncomingFromIPU and IncomingFromOffnet**

Step 12 Create Partition to CSS mappings for the created CSSs

Step 13 Create a **GL-DP-Trunk** device pool

Step 14 Create a **location-bvsm** location

Step 15 Create a gatekeeper, for example **10.120.2.51**

Step 16 Create H.225 Trunks (Gatekeeper Controlled): **e2c1-External, e2c1-Offnet and e2c1-Vmail**

Step 17 Reset the H.225 Trunks

Step 18 Create Route Groups: **EXTERNAL, OFFNETTRUNK** and **VOICEMAIL**

Step 19 Route Lists: **INTERSITE** and **INTRASITE, OFFNETTRUNK** and **VOICEMAIL**

Add Country Transactions

This section has two topics:

- Add Country Transaction on PGW, page D-20
- Add Country Transaction on Unified CM, page D-20

Add Country Transaction on PGW

USM invokes the PGW driver and uses the mml scripts in the AddCountryTransits transaction of the PGW MML model worksheet to:

Step 1 Configure the CTRY dial plan with country specific information

Step 2 Create and configure country specific dial plans on the PGW as follows:

- E#PADDEDCC# dial plan, for example **E044**
- F#PADDEDCC# dial plan, for example **F044**
- H#PADDEDCC# dial plan, for example **H044**
- L#PADDEDCC# dial plan, for example **L044**
- N#PADDEDCC# dial plan, for example **N044**
- P#PADDEDCC# dial plan, for example **P044**
- R#PADDEDCC# dial plan, for example **R044**
- S#PADDEDCC# dial plan, for example **S044**

Step 3 Configure the **ILGW dial plan** with country specific information.

Add Country Transaction on Unified CM

USM invokes the CCM7.1.x drivers and uses the definitions in the AddCountry transaction of the CCM model worksheet to create and configure on all Unified CM Clusters:

- Country Specific Route Lists; for example, **PSTNNAT044, PSTNINT044**, and **EMERGENCY044**
- Associate country specific Route Lists to the **EXTERNAL** Route Group

Add Customers Transaction

USM invokes the PGW 9.6.1 driver and uses the mml scripts in the AddCustomer transaction of the PGW MML model worksheet.

Procedure:

Step 1 Add and configure customer specific dial plans on the PGW as follows:

- Per-customer Ingress dial plan (#CUSTDIALPLAN#), for example **0001**

- Per-customer Egress dial plan (#EGRESSCUSTDIALPLAN#), for example **0002**
- Per-customer Egress dial plan 2 (#EGRESSCUSTDIALPLAN2#), for example **0003**
- Per-customer Central Legacy PBX dial plan (#COMMONLEGACYPBX#), for example **0004**

Step 2 Configure the core ICCM and ROUT dial plans with customer specific information.

Add Locations Transactions

The following two topics are explianed in this section:

- Add Locations Transaction on PGW
- Add Locations Transaction on Unified CM

Add Locations Transaction on PGW

USM invokes the PGW 9.6.1 driver and uses the mml scripts in the AddLocationFirstInCountry and AddLocation transactions of the PGW_9_6_1 model worksheet.

Procedure:

Step 1 Configure the AddLocationFirstInCountry transaction as follows:

- Per-customer Ingress (#CUSTDIALPLAN#) dial plan, for example **0001**
- Per-customer Egress 2 (#EGRESSCUSTDIALPLAN2#) dial plan, for example **0003**
- with location specific information. This transaction is executed for each first location per Country and per Customer.

Step 2 Configure the AddLocation transaction as follows:

- Per-customer Ingress (#CUSTDIALPLAN#) dial plan, for example **0001**
- Per-customer Egress (#EGRESSCUSTDIALPLAN#) dial plan, for example **0002**
- Per-customer Egress 2 (#EGRESSCUSTDIALPLAN2#) dial plan, for example **0003**
- Per-country R#PADDEDCC# dial plan, for example **R044**
- Core ROUT dial plan

Add Locations Transaction on Unified CM

USM invokes the CCM drivers and uses the definitions in the AddLocation transaction of the CCM model worksheet to create and configure on the selected Unified CM Cluster (Generic Hosted UCS 7.1(a) model is shown below):

- Site specific location, for example **location-bvsm-1**
- 55 Per-location Partitions (Call Routing, Internal, 24x7, Standard Business Hours, Extended Business Hours, Weekend, Call Blocking, Call Forwarding and CLIR partitions), for example **AllowInternal1, Site1, AllowPSTNServices24Hour1, AllowInterSiteCF1**, etc

- 36 Per-location CSSs (Static, Incoming Call, Phone, Line, Per COS, Presence CSSs and CLIR CSSs), for example **TempOutOfServiceCSS1, IncomingToSite1, EmergencyOnly1, COS1International24Hour1, InternalCF, SUBSCRIBE**, etc
- Partition to CSS mappings for the created CSSs
- 7 Per-location Generic Route Patterns, for routing basic calls, and call forwarding, for example **1000100!, 8.!, [^89]XX,** etc
- 4 Generic Translation Patterns, for example **1000100!, [^89]XX, 9999991000100111.!**
- Number of Country Specific per-location Route Patterns and Translation Patterns
- 2 Device pools for phones and faxes, for example **devicepool1** and **faxdevicepool1**

Move Phone Inventory Transaction

USM invokes the IPPBX driver on the selected Unified CM Cluster to do the following:

Step 1 verify that the phone is not already configured (removePhone), for example

<phoneName>**SEP001D452CDA84**</phoneName>

Step 2 Add a new phone (addPhone), for example:

<newPhone>

<name>**SEP001D452CDA84**</name>

<product>**Cisco 7965**</product>

<model>**Cisco 7965**</model>

<class>**Phone**</class>

<protocol>**SIP**</protocol>

<protocolSide>User</protocolSide>

<devicePoolName>**devicepool1**</devicePoolName>

<numberOfButtons>**6**</numberOfButtons>

<phoneTemplateName>**Standard 7965 SIP**</phoneTemplateName>

</newPhone>

Note The next step is only executed on Unified CM 5.x clusters, since autogenerated device profiles are not used in Unified CM 6.x

Step 3 Create an autogenerated profile for the phone (createAutogeneratedProfile), for example:

<phoneName>SEP001D452CDA84</phoneName>

Step 4 add a new line to the phone (addLine), for example:

<newLine>

<pattern>**88810001001110000**</pattern>

<description>**Line 88810001001110000 for a phone**</description>

<usage>Device</usage>

<routePartitionName>**Site1**</routePartitionName>

<callForwardAll>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardAll>

<callForwardBusy>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardBusy>

<callForwardBusyInt>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardBusyInt>

<callForwardNoAnswer>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswer>

<callForwardNoAnswerInt>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswerInt>

<callForwardNoCoverage>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverage>

<callForwardNoCoverageInt>

<callingSearchSpaceName>**BlockAllCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverageInt>

<autoAnswer>Auto Answer Off</autoAnswer>

<networkHoldMOHAudioSourceId></networkHoldMOHAudioSourceId>

<userHoldMOHAudioSourceId></userHoldMOHAudioSourceId>

<shareLineAppearanceCSSName>**COS6InternalCLIP24Hour1**</shareLineAppearanceCSSName>

<voiceMailProfileName></voiceMailProfileName>

</newLine>

Step 5 update the phone (updatePhone), for example:

<name>**SEP001D452CDA84**</name>

```
<callingSearchSpaceName>EmergencyOnly1</callingSearchSpaceName>
<devicePoolName>devicepool1</devicePoolName>
<locationName>location-bvsm-1</locationName>
<networkHoldMOHAudioSourceId>0</networkHoldMOHAudioSourceId>
<userHoldMOHAudioSourceId>0</userHoldMOHAudioSourceId>
<aarNeighborhoodName></aarNeighborhoodName>
<vendorConfig>
    <disableSpeaker>false</disableSpeaker>
    <disableSpeakerAndHeadset>false</disableSpeakerAndHeadset>
    <forwardingDelay>0</forwardingDelay>
    <pcPort>0</pcPort>
    <settingsAccess>1</settingsAccess>
    <garp>1</garp>
    <voiceVlanAccess>1</voiceVlanAccess>
    <videoCapability>0</videoCapability>
    <autoSelectLineEnable>0</autoSelectLineEnable>
    <webAccess>0</webAccess>
</vendorConfig>
<lines>
    <line uuid="{e1cd8b3a-c74c-1053-1494-bd06fafd4a90}" index="1">
    <label>88810001002120000</label>
    <display>88810001002120000</display>
    <dirn uuid="{e1cd8b3a-c74c-1053-1494-bd06fafd4a90}"></dirn>
    <ringSetting>Use System Default</ringSetting>
    <consecutiveRingSetting>Use System Default</consecutiveRingSetting>
    <e164Mask></e164Mask>
    <maxNumCalls>1</maxNumCalls>
    <busyTrigger>1</busyTrigger>
    <mwlPolicy>Use System Policy</mwlPolicy>
    </line>
</lines>
<phoneTemplateName>Standard 7965 SIP</phoneTemplateName>
<speeddials></speeddials>
<userLocale>English United States</userLocale>
<networkLocale>United States</networkLocale>
<deviceSecurityMode>Use System Default</deviceSecurityMode>
<idleTimeout>0</idleTimeout>
<services>
```

<service uuid="{be4d6290-f402-dc20-1717-55510000fcb5}">

<telecasterServiceName>**Phone Services**</telecasterServiceName>

<name>**Phone Services**</name>

<url>**http://10.120.3.66:8080/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#**</url>

<urlButtonIndex>**0**</urlButtonIndex>

<urlLabel>**Phone Services**</urlLabel>

</service>

</services>

<softkeyTemplateName>Standard Feature</softkeyTemplateName>

<enableExtensionMobility>false</enableExtensionMobility>

<builtInBridgeStatus>Off</builtInBridgeStatus>

<callInfoPrivacyStatus>Off</callInfoPrivacyStatus>

<ignorePresentationIndicators>false</ignorePresentationIndicators>

<packetCaptureMode>None</packetCaptureMode>

<packetCaptureDuration>0</packetCaptureDuration>

Step 6 Reset the phone (doDeviceReset), for example:

<deviceName>**SEP001D452CDA84**</deviceName>

<isHardReset>**true**</isHardReset>

Add PSTN Published Number Transaction

USM invokes the PGW 9.6.1 driver and uses the mml scripts in the AddPSTNPubNum transaction of the PGW model worksheet to do the following:

- Edit the relevant digmodstrings in the per-customer Ingress dial plan (#CUSTDIALPLAN#, for example **0001**) with the configured PSTN Published number

Add Emergency Published Number Transaction

USM invokes the PGW9.6.1 driver and uses the mml scripts in the AddEmergNum transaction of the PGW_9_6_1 model worksheet to do the following:

- Configure the per-customer Ingress dial plan (#CUSTDIALPLAN#, for example **0001**) for the correct routing and number presentation of emergency calls from the relevant location.

Assign Range of E164 Numbers to Internal Numbers Transactions

Starting from Hosted UCS 6.1(a) USM invokes the PGW TimesTen driver and uses the TimesTen Input in the AssocaiteFNN transaction (AssociateFNN script) of the PGW_TimesTen_Any model worksheet to create an import file and transfer it to the PGW, where it invokes the HUCSprovx10 PGW script and inserts the associations into the PGW TimesTen database.

Following is a sample Input file for 5 DDI mappings (1630411000-1630411004) generated for the HUCSprovx10 PGW script:

FNT,0001cr9fnt,2,00100109411000,E441630411000

FNT,0002afnt,2,441630411000,F8411000

FNT,r001bfnt,1,441630411000,0010010411000

FNT,0001cr9fnt,2,00100109411001,E441630411001

FNT,0002afnt,2,441630411001,F8411001

FNT,r001bfnt,1,441630411001,0010010411001

FNT,0001cr9fnt,2,00100109411002,E441630411002

FNT,0002afnt,2,441630411002,F8411002

FNT,r001bfnt,1,441630411002,0010010411002

FNT,0001cr9fnt,2,00100109411003,E441630411003

FNT,0002afnt,2,441630411003,F8411003

FNT,r001bfnt,1,441630411003,0010010411003

FNT,0001cr9fnt,2,00100109411004,E441630411004

FNT,0002afnt,2,441630411004,F8411004

FNT,r001bfnt,1,441630411004,0010010411004

Register Phone Transaction

USM invokes the IPPBX driver on the selected Unified CM Cluster to do the following:

Step 1 Delete the old line (created when the phone was moved to a location), and add a new line to the phone (addLine), for example:

<newLine>

<pattern>**10001002120201**</pattern>

<description>**Line 10001002120201 for a phone**</description>

<usage>Device</usage>

<routePartitionName>**Site1**</routePartitionName>

<callForwardAll>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardAll>

<callForwardBusy>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardBusy>

<callForwardBusyInt>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardBusyInt>

<callForwardNoAnswer>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswer>

<callForwardNoAnswerInt>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswerInt>

<callForwardNoCoverage>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverage>

<callForwardNoCoverageInt>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverageInt>

<autoAnswer>Auto Answer Off</autoAnswer>

<networkHoldMOHAudioSourceId></networkHoldMOHAudioSourceId>

<userHoldMOHAudioSourceId></userHoldMOHAudioSourceId>

<shareLineAppearanceCSSName>**COS1International24Hour1**</shareLineAppearanceCSSName>

<voiceMailProfileName></voiceMailProfileName>

</newLine>

Step 2 Update the phone (updatePhone), for example:

<name>**SEP001D452CDA84**</name>

<callingSearchSpaceName>**EmergencyOnly1**</callingSearchSpaceName>

<devicePoolName>**devicepool1**</devicePoolName>

<locationName>**location-bvsm-1**</locationName>

<networkHoldMOHAudioSourceId>0</networkHoldMOHAudioSourceId>

```xml
<userHoldMOHAudioSourceId>0</userHoldMOHAudioSourceId>
<aarNeighborhoodName></aarNeighborhoodName>
<vendorConfig>
    <disableSpeaker>false</disableSpeaker>
    <disableSpeakerAndHeadset>false</disableSpeakerAndHeadset>
    <forwardingDelay>1</forwardingDelay>
    <pcPort>0</pcPort>
    <settingsAccess>1</settingsAccess>
    <garp>1</garp>
    <voiceVlanAccess>1</voiceVlanAccess>
    <videoCapability>0</videoCapability>
    <autoSelectLineEnable>0</autoSelectLineEnable>
    <webAccess>0</webAccess>
</vendorConfig>
<lines>
    <line uuid="{e1cd8b3a-c74c-1053-1494-bd06fafd4a90}" index="1">
    <label>Desk4</label>
    <display>Desk4</display>
    <dirn uuid="{e1cd8b3a-c74c-1053-1494-bd06fafd4a90}"></dirn>
    <ringSetting>Use System Default</ringSetting>
    <consecutiveRingSetting>Use System Default</consecutiveRingSetting>
    <e164Mask>1631111001</e164Mask>
    <maxNumCalls>4</maxNumCalls>
    <busyTrigger>2</busyTrigger>
    <mwlPolicy>Use System Policy</mwlPolicy>
    </line>
</lines>
<phoneTemplateName>Standard 7965 SIP</phoneTemplateName>
<speeddials></speeddials>
<userLocale>English United States</userLocale>
<networkLocale>United States</networkLocale>
<deviceSecurityMode>Use System Default</deviceSecurityMode>
<idleTimeout>0</idleTimeout>
<services>
    <service uuid="{be4d6290-f402-dc20-1717-55510000fcb5}">
    <telecasterServiceName>Login/Logout</telecasterServiceName>
    <name>Login/Logout</name>
    <url>http://10.132.4.2:8080/emapp/EMAppServlet?device=#DEVICENAME#</url>
```

<urlButtonIndex>0</urlButtonIndex>

<urlLabel>**Login/Logout**</urlLabel>

<telecasterServiceName>**Phone Services**</telecasterServiceName>

<name>**Phone Services**</name>

<url>**http://10.120.3.66:8080/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#**</url>

<urlButtonIndex>0</urlButtonIndex>

<urlLabel>**Phone Services**</urlLabel>

</service>

</services>

<softkeyTemplateName>**Softkey_Advanced**</softkeyTemplateName>
<defaultProfileName>**ADP001D452CDA84**</defaultProfileName> [see Note]

<enableExtensionMobility>**true**</enableExtensionMobility>

<builtInBridgeStatus>Off</builtInBridgeStatus>

<callInfoPrivacyStatus>Off</callInfoPrivacyStatus>

<ignorePresentationIndicators>false</ignorePresentationIndicators>

<packetCaptureMode>None</packetCaptureMode>

<packetCaptureDuration>0</packetCaptureDuration>

Note The <defaultProfileName> is only executed on Unified CM 5.x clusters, since autogenerated device profiles are not used in Unified CM 6.x

Step 3 Reset the phone (doDeviceReset), for example:

<deviceName>**SEP001D452CDA84**</deviceName>

<isHardReset>**true**</isHardReset>

Add End User Transaction

USM invokes the IPPBX driver on the selected Unified CM Cluster to do the following:

Add the user (addUser), for example:

<addUser>

<firstname>**FirstName**</firstname>

<lastname>**LastName**</lastname>

<userid>**clu1cus1loc1user1**</userid>

<password>********</password>

<pin>*****</pin>

<telephoneNumber></telephoneNumber>

<department></department>

</addUser>

Add User Extension Mobility Transaction

USM invokes the IPPBX driver on the selected Unified CM Cluster to do the following:

Step 1 Add a device profile (addDeviceProfile), for example:

<addDeviceProfile>
<name>**clu1cus1loc1user1**</name>
<product>**Cisco 7961**</product>
<model>**Cisco 7961**</model>
<class>Phone</class>
<protocol>**SCCP**</protocol>
<protocolSide>User</protocolSide>
<devicePoolName>**devicepool1**</devicePoolName>
<numberOfButtons>**6**</numberOfButtons>
<phoneTemplateName>**Standard 7961 SCCP**</phoneTemplateName>
</addDeviceProfile>

Step 2 Add a new line (addLine), for example:

<newLine>
<pattern>**1000100111202**</pattern>
<description>**Line 1000100111202 for a phone**</description>
<usage>Device</usage>
<routePartitionName>**Site1**</routePartitionName>
<callForwardAll>
<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>
<destination></destination>
</callForwardAll>
<callForwardBusy>
<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>
<destination></destination>
</callForwardBusy>
<callForwardBusyInt>
<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>
<destination></destination>
</callForwardBusyInt>
<callForwardNoAnswer>
<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswer>

<callForwardNoAnswerInt>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoAnswerInt>

<callForwardNoCoverage>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverage>

<callForwardNoCoverageInt>

<callingSearchSpaceName>**PSTNIntMobCF1**</callingSearchSpaceName>

<destination></destination>

</callForwardNoCoverageInt>

<autoAnswer>Auto Answer Off</autoAnswer>

<networkHoldMOHAudioSourceId></networkHoldMOHAudioSourceId>

<userHoldMOHAudioSourceId></userHoldMOHAudioSourceId>

<shareLineAppearanceCSSName>**COS1International24Hour1**</shareLineAppearanceCSSName>

<voiceMailProfileName></voiceMailProfileName>

</newLine>

Step 3 Update the created device profile (updateDeviceProfile), for example:

<name>clu1cus1loc1user1</name>

<lines>

<line uuid="{f7829840-69b4-1bf6-13ca-884a93cb2195}" index="1">

<label>**1631111202**</label>

<display></display>

<dirn uuid="{f7829840-69b4-1bf6-13ca-884a93cb2195}"></dirn>

<ringSetting>Use System Default</ringSetting>

<consecutiveRingSetting>Use System Default</consecutiveRingSetting>

<e164Mask>**1631111202**</e164Mask>

<maxNumCalls>**4**</maxNumCalls>

<busyTrigger>**2**</busyTrigger>

<mwlPolicy>Use System Policy</mwlPolicy>

</line>

</lines>

<phoneTemplateName>**Standard 7961 SCCP**</phoneTemplateName>

<speeddials></speeddials>

<userLocale>English United States</userLocale>

<services>

<service uuid="{7f7c00ca-3ff5-73b6-60fc-caeac54ac430}">

<telecasterServiceName>Login/Logout</telecasterServiceName>

<name>**Login/Logout**</name>

<url>**http://10.132.4.2:8080/emapp/EMAppServlet?device=#DEVICENAME#**</url>

<urlButtonIndex>0</urlButtonIndex>

<urlLabel>**Login/Logout**</urlLabel>

</service>

<service uuid="{be4d6290-f402-dc20-1717-55510000fcb5}">

<telecasterServiceName>**Phone Services**</telecasterServiceName>

<name>Phone Services</name>

<url>**http://10.120.3.66:8080/bvsmweb/bvsmservices.cgi?device=#DEVICENAME#**</url>

<urlButtonIndex>0</urlButtonIndex>

<urlLabel>**Phone Services**</urlLabel>

</service>

</services>

<softkeyTemplateName>**Softkey_Advanced**</softkeyTemplateName>

<ignorePresentationIndicators>false</ignorePresentationIndicators>

Step 4 Update the user (updateUser), for example:

<userid>**clu1cus1loc1user1**</userid>

<phoneProfiles>

<profileName>**clu1cus1loc1user1**</profileName>

</phoneProfiles>

Configure BO2OT for Customer Transaction

USM invokes the PGW driver and uses the EnableBO2OCT mml script (AddCustomer transaction) of the PGW model worksheet to do the following:

Configure the per-customer Egress Dial Plan 2 #EGRESSCUSTDIALPLAN2# to Mark Incoming OffNet calls.

Example:

;EnableBO2OCT

; 0007 - Per Customer Egress Dial Plan 2

numan-ed:anoa:custgrpid="0007",setname="MarkBnumOffnet",noavalue=4

numan-ed:anoa:custgrpid="0007",setname="MarkBnumOffnet",noavalue=5

Add Overlay Area Codes Transaction

USM invokes the CCM6.1.x drivers and uses the definitions in the AddLocation transaction of the CCM model worksheet to create and configure on the selected CUCM Cluster (Generic HUCS 5.1(B) model).

9 US specific per-location translation Patterns for 10-digit (invoked by the LocationLocalArea-10 model) Local Dialling support: USALocalCalls24Hour, USALocalCLIOCalls24Hour, USALocalCallsStd, USALocalCLIOCallsStd, USALocalCallsExt, USALocalCLIOCallsExt, USALocalCallsWend, USALocalCLIOCallsWend, and USALocalCallsCF

APPENDIX E

Local Gateway Supported Call Scenarios

Revised: 08/12/2010, OL-23270-01

This document describes the Local Gateway supported call scenarios in Cisco Hosted UCS. In the Hosted UCS 7.1.1 lite release, following call flows are supported:

Outgoing PSTN Calls

This section has the following topics:

Non-Emergency calls (CgPN and CdPN NOA setting)

For all of the Non-Emergency calls the CgPN and CdPN can be sent to the PSTN differently depending on how the trunk is configured to handle NOA. Therefore, following Non-Emergency outgoing PSTN calls are supported:

- CgPN NOA is set (Yes), CdPN is set (Yes)
- CgPN NOA is set (Yes), CdPN is not set (No)
- CgPN NOA is not set (No), CdPN is set (Yes)
- CgPN NOA is not set (No), CdPN is not set (No)

IP Phone -> PSTN (Any Non-Emergency PSTN Call, CdPN NOA - Yes; CgPN NOA - Yes)

In this call scenario:

- CdPN NOA is set (Yes)

- CgPN NOA is set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-1 IP Phone -> PSTN (CdPN NOA - Yes; CgPN NOA - Yes)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 00	CdPN: 314-5550003 (Nat) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (Any Non-Emer PSTN Call, CdPN NOA - Yes; CgPN NOA - No)

In this call scenario:

CdPN NOA is set (Yes)

CgPN NOA is not set (No)

IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-2 IP Phone -> PSTN (CdPN NOA - Yes; CgPN NOA - No)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) CgPN: NAC1 + E164N1 (Unk)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) CgPN: 1 + 212-5550001 (Unk)

IP Phone -> PSTN (Any Non-Emer PSTN Call, CdPN NOA - No; CgPN NOA - Yes)

In this call scenario:

CdPN NOA is not set (No)

CgPN NOA is set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-3 IP Phone -> PSTN (CdPN NOA - No; CgPN NOA - Yes)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: NAC1 + E164N3 (Unk) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 1 + 314-5550003 (Unk) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (Any Non-Emer PSTN Call, CdPN NOA - No; CgPN NOA - No)

In this call scenario:

- CdPN NOA is not set (No)
- CgPN NOA is not set (No)
- IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-4 IP Phone -> PSTN (CdPN NOA - No; CgPN NOA - No)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: NAC1 + E164N3 (Unk) CgPN: NAC1 + E164N1 (Unk)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 1 + 314-5550003 (Unk) CgPN: 1 + 212-5550001 (Unk)

Non-Emergency Calls (With and Without DDI)

For all of the above calls the CgPN is processed differently depending on whether the line has an E.164 number associated with the internal number. Therefore, following Non-Emergency outgoing PSTN calls are supported:

- User line configured with DDI,
- User line configured without DDI.

IP Phone (with DDI) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-5 IP Phone (with DDI) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + 9 + SLC1 + EXT1	CdPN: E164N3 (Nat) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) CgPN: 212-5550001 (Nat)

IP Phone (without DDI) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, without DDI Number) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-6 IP Phone (without DDI) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) CgPN: E164N0 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) CgPN: 212-5550000 (Nat)

Non-Emergency Calls (CLIR/CLIP)

For all of the above calls the Presentation Indicator is setup differently depending on whether the user has made a call from a location configured as CLIR or CLIP, and whether the user has made a call using the CLIR or CLIP release code. Therefore, following Non-Emergency outgoing PSTN calls are supported:

- User dialing from a location configured as CLIR,
- User dialing from a location configured as CLIR and using CLIR release code,
- User dialing from a location configured as CLIP,
- User dialing from a location configured as CLIP and using CLIP release code.

IP Phone (CLIR) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 configured as LPS1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-7 IP Phone (CLIR) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1 (CLIR)	CdPN: 90 + E164N3 (PI LPS1) CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) (PI LPS1) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 (PI restricted) CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) (PI restricted) CgPN: 212-5550001 (Nat)

IP Phone (CLIR Release) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

CdPN NOA is for example set (Yes)

CgPN NOA is for example set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 configured as LPS1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 and using CCRC1 (Dialed number: PAP1 + CCRC1 + NAC1 + E164N3)

Figure E-8 IP Phone (CLIR Release) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + CCRC1 + NAC1 + E164N3 CgPN: SLC1 + EXT1 (CLIR)	CdPN: 90 + E164N3 (PI LPS2) CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) (PI LPS2) CgPN: E164N1 (Nat)
CdPN: 9 + *82 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 (PI allowed) CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) (PI allowed) CgPN: 212-5550001 (Nat)

IP Phone (CLIP) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 configured as LPS2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-9 IP Phone (CLIP) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1 (CLIR)	CdPN: 90 + E164N3 (PI LPS2) CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) (PI LPS2) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 (PI allowed) CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) (PI allowed) CgPN: 212-5550001 (Nat)

IP Phone (CLIP Release) -> PSTN (Any non-Emergency PSTN Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 configured as LPS2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Non-Emergency call, for example a National (Long-distance) call to E164N3 and using CCRC2 (Dialed number: PAP1 + CCRC2 + NAC1 + E164N3)

Figure E-10 IP Phone (CLIP Release) -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + CCRC2 + NAC1 + E164N3 CgPN: SLC1 + EXT1 (CLIR)	CdPN: 90 + E164N3 (PI LPS1) CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) (PI LPS1) CgPN: E164N1 (Nat)
CdPN: 9 + *67 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 (PI restricted) CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) (PI restricted) CgPN: 212-5550001 (Nat)

Non-Emergency Calls (Nat, Int, Premium, Service, Free, Loc)

Following Non-Emergency outgoing PSTN calls are supported:

- National,
- International,
- Premium,
- Service,
- Free Phone,
- Local.

IP Phone -> PSTN (National Call)

In this call scenario:

CdPN NOA is for example set (Yes)

CgPN NOA is for example set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a National (Long-distance) call to E164N3 (Dialed number: PAP1 + NAC1 + E164N3)

Figure E-11 IP Phone -> PSTN (National Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164N3 (Nat) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 314-5550003 (Nat) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (International Call)

In this call scenario:

CdPN NOA is for example set (Yes)

CgPN NOA is for example set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making an International call to E164I5 (Dialed number: PAP1 + IAC1 + E164I5)

Figure E-12 IP Phone -> PSTN (International Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + IAC1 + E164I5 CgPN: SLC1 + EXT1	CdPN: 900 + E164I5 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: E164I5 (Int) CgPN: E164N1 (Nat)
CdPN: 9 + 011 + 44-1632-123456 CgPN: 431 + 0001	CdPN: 900 + 44-1632-123456 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 44-1632-123456 (Int) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (Premium Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Premium call to PREM (Dialed number: PAP1 + NAC1 + PREM)

Figure E-13 IP Phone -> PSTN (Premium Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + PREM CgPN: SLC1 + EXT1	CdPN: 90 + PREM CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: PREM (Nat) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 900-NXXXXXX CgPN: 431 + 0001	CdPN: 90 + 900-NXXXXXX CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 900-NXXXXXX (Nat) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (Service Call)

In this call scenario:

CdPN NOA is for example set (Yes)

CgPN NOA is for example set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Service call to N11S (Dialed number: PAP1 + N11S)

Figure E-14 IP Phone -> PSTN (Service Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + N11S CgPN: SLC1 + EXT1	CdPN: 9090000 + N11S CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: N11S (Unk) CgPN: E164N1 (Nat)
CdPN: 9 + 411 CgPN: 431 + 0001	CdPN: 9090000 + 411 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 411 (Unk) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (Toll-free Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a Toll-free call to FREE (Dialed number: PAP1 + NAC1 + FREE)

Figure E-15 IP Phone -> PSTN (Toll-free Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + FREE CgPN: SLC1 + EXT1	CdPN: 90 + FREE CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: FREE (Nat) CgPN: E164N1 (Nat)
CdPN: 9 + 1 + 800-NXXXXXX CgPN: 431 + 0001	CdPN: 90 + 800-NXXXXXX CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 800-NXXXXXX (Nat) CgPN: 212-5550001 (Nat)

IP Phone -> PSTN (7-digit Local Call, send NDC)

In this call scenario:

- LGW Trunk is configured to set the NDC for Local Calls
- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC2 + EXT1, DDI Number: NDC3 + SN3) in Location 2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID2) is making a 7-digit local call to SN4 (Dialed number: PAP1 + SN4)

Figure E-16 IP Phone -> PSTN (7-digit Local Call, send NDC)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + SN4 CgPN: SLC2 + EXT1	CdPN: 90 + NDC3 + SN4 CgPN: CPID1 + RID2 + CT + SLC2 + EXT1	CdPN: NDC3 + SN4 (Sub) CgPN: NDC3 + SN3 (Sub)
CdPN: 9 + 5550004 CgPN: 432 + 0001	CdPN: 90 + 314 + 5550004 CgPN: 220 + 0100 + 9 + 432 + 0001	CdPN: 314 + 5550004 (Sub) CgPN: 314 + 5550003 (Sub)

IP Phone -> PSTN (7-digit Local Call, don't send NDC)

In this call scenario:

- LGW Trunk is configured not to set the NDC for Local Calls
- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC2 + EXT1, DDI Number: NDC3 + SN3) in Location 2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID2) is making a 7-digit local call to SN4 (Dialed number: PAP1 + SN4)

Figure E-17 IP Phone -> PSTN (7-digit Local Call, don't send NDC)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + SN4 CgPN: SLC2 + EXT1	CdPN: 90 + NDC3 + SN4 CgPN: CPID1 + RID2 + CT + SLC2 + EXT1	CdPN: SN4 (Sub) CgPN: SN3 (Sub)
CdPN: 9 + 5550004 CgPN: 432 + 0001	CdPN: 90 + 314 + 5550004 CgPN: 220 + 0100 + 5 + 432 + 0001	CdPN: 5550004 (Sub) CgPN: 5550003 (Sub)

IP Phone -> PSTN (10-digit Local Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: NDC1 + SN1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a 10-digit local call to NDC1 + SN2 (Dialed number: PAP1 + NDC1 + SN2)

Figure E-18 IP Phone -> PSTN (10-digit Local Call))

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NDC1 + SN2 CgPN: SLC1 + EXT1	CdPN: 90 + NDC1 + SN2 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: NDC1 + SN2 (Sub) CgPN: NDC1 + SN1 (Sub)
CdPN: 9 + 212 + 5550002 CgPN: 431 + 0001	CCdPN: 90 + 212+ 5550002 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 212 + 5550002 (Sub) CgPN: 212 + 5550001 (Sub)

IP Phone -> PSTN (11-digit Local Call)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, DDI Number: NDC1 + SN1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1) is making a 11-digit local call to NDC1 + SN2 (Dialed number: PAP1 + NDC1 + SN2)

Figure E-19 IP Phone -> PSTN (11-digit Local Call)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + NDC1 + SN2 CgPN: SLC1 + EXT1	CdPN: 90 + NDC1 + SN2 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: NDC1 + SN2 (Sub) CgPN: NDC1 + SN1 (Sub)
CdPN: 9 + 1 + 212 + 5550002 CgPN: 431 + 0001	CdPN: 90 + 212+ 5550002 CgPN: 220 + 0010 + 9 + 431 + 0001	CdPN: 212 + 5550002 (Sub) CgPN: 212 + 5550001 (Sub)

IP Phone -> IntraSite -> IP Phone -> Call Forward -> PSTN

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone 1 (Internal Number: SLC1 + EXT1, DDI Number: E164N1)) is making an Intra-site call to IP Phone 2 (Internal Number: SLC1 + EXT2, DDI Number: E164N2) both in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1. IP Phone 2 has CFA set to E164N3

Note IP Phone > IntraSite > IP Phone call processing is not shown since there is no difference if Local PSTN Access is used

Figure E-20 IP Phone -> IntraSite -> IP Phone -> Call Forward -> PSTN)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: EXT1 RdN: SLC1 + EXT2	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + SLC1 + EXT1 RdN: SLC1 + EXT2	CdPN: E164N3 (Nat) CgPN: E164N0 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 0001 RdN: 431 + 0002	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 5 + 431 + 0001 RdN: 431 + 0002	CdPN: 314-5550003 (Nat) CgPN: 212-5550000 (Nat)

IP Phone -> InterSite -> IP Phone -> Call Forward -> PSTN

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone 1 (Internal Number: SLC1 + EXT1, DDI Number: E164N1)) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1 is making an Inter-site call to IP Phone 2 (Internal Number: SLC2 + EXT1, DDI Number: E164N3) in Location 2 on Unified CM cluster 1 (PSTN Published Number: E164N07, Unified CM ID: CPID1, Location RID: RID2. IP Phone 2 has CFA set to E164N2

Note IP Phone > InterSite > IP Phone call processing is not shown since there is no difference if Local PSTN Access is used

Figure E-21 IP Phone -> InterSite -> IP Phone -> Call Forward -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N2 CgPN: ISP + SLC1 + EXT1 RdN: SLC2 + EXT1	CdPN: 90 + E164N2 CgPN: CPID1 + RID2 + CT + SLC1 + EXT1 RdN: SLC2 + EXT1	CdPN: E164N2 (Nat) CgPN: E164N07 (Nat)
CdPN: 9 + 1 + 646-5550002 CgPN: 8 + SLC1 + 0001 RdN: 432 + 0001	CdPN: 90 + 646-5550002 CgPN: 220 + 0100 + 5 + 431 + 0001 RdN: 432 + 0001	CdPN: 646-5550002 (Nat) CgPN: 314-5550000 (Nat)

PSTN -> IP Phone -> Call Forward -> PSTN

In this call scenario:

- CdPN NOA is for example set (Yes)

- CgPN NOA is for example set (Yes)
- PSTN user (E.164 number: PSTN) is making a call to IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1)) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1. IP Phone has CFA set to E164N3

Note PSTN > IP Phone call processing is not shown since as it is described in the next section

Figure E-22 IPSNT -> IP Phone -> Call Forward -> PSTN

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: PAP1 + NAC1 + E164N3 CgPN: PAP1 + NAC1 + PSTN RdN: SLC1 + EXT1	CdPN: 90 + E164N3 CgPN: CPID1 + RID1 + CT + PAP1 + NAC1 + PSTN RdN: SLC1 + EXT2	CdPN: E164N3 (Nat) CgPN: E164N0 (Nat)
CdPN: 9 + 1 + 314-5550003 CgPN: 9 + 1 + 214-5551234 RdN: 431 + 0001	CdPN: 90 + 314-5550003 CgPN: 220 + 0010 + 5 + 9 + 1 + 214-5551234 RdN: 431 + 0001	CdPN: 314-5550003 (Nat) CgPN: 212-5550000 (Nat)

Emergency calls

For outgoing Emergency calls:

- If the location is not configured to use the "Cisco Emergency Responder" or "DDI for Emergency" feature, the CgPN will always be replaced with the Location Emergency Published Number.
- If the location is configured to use the "Cisco Emergency Responder" feature, the CgPN number is modified to the Emergency Location Identification Number (ELIN).
- If the location is configured to use the "DDI for Emergency" feature, the CgPN will be replaced with an E.164 number of the line which originated the call (if the line is associated with an E.164 number) or with the Location Emergency Published Number (if the line is not associated with an E.164 number).

Therefore, following Emergency outgoing PSTN calls are supported:

- IP Phone -> PSTN (Emergency Call, Default handling),
- IP Phone -> PSTN (Emergency Call, Cisco ER configured),
- IP Phone (with DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled),
- IP Phone (without DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

For all of the above calls the Presentation Indicator is not setup differently regardless of whether the user has made a call from a location configured as CLIR or CLIP, and whether the user has made a call using the CLIR or CLIP release code.

IP Phone -> PSTN (Emergency Call, Default handling)

In this call scenario:

CdPN NOA is for example set (Yes)

CgPN NOA is for example set (Yes)

IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, Default Emergency Call Handling) is making an Emergency call to EMER (Dialed number: EMER)

Figure E-23 IP Phone -> PSTN (Emergency Call, Default handling)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: EMER CgPN: SLC1 + EXT1	CdPN: 9 + EMER CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: EMER (Unk) CgPN: E164N0 (Nat)
CdPN: 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 220 + 0010 + 4 + 431 + 0001	CdPN: 911 (Unk) CgPN: 212-5550000 (Nat)

IP Phone -> PSTN (Emergency Call, Cisco ER configured)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, Cisco ER Configured) is making an Emergency call to EMER (Dialed number: EMER). IP Phone is for example in ERL1 (configured with ELIN1).

Figure E-24 IP Phone -> PSTN (Emergency Call, Cisco ER configured)

Unified CM IN	Unified CM OUT - CER IN	CER OUT - Unified CM IN
CdPN: EMER CgPN: SLC1 + EXT1	CdPN: EMER CgPN: SLC1 + EXT1	CdPN: CERID + ELIN1 + EMER CgPN: SLC1 + EXT1
CdPN: 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 431 + 0001	CdPN: 1 + 212-9110000 + 911 CgPN: 431 + 0001
Unified CM IN	**Unified CM OUT - LGW IN**	**LGW OUT**
CdPN: CERID + ELIN1 + EMER CgPN: SLC1 + EXT1	CdPN: 9 + EMER CgPN: CPID1 + RID1 + CT + ELIN1	CdPN: EMER (Unk) CgPN: ELIN1 (Nat)
CdPN: 1 + 212-9110000 + 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 220 + 0010 + 4 + 212-9110000	CdPN: 911 (Unk) CgPN: 212-9110000 (Nat)

IP Phone (with DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, "DDI for Emergency" enabled) is making an Emergency call to EMER (Dialed number: EMER)

Figure E-25 IP Phone (with DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: EMER CgPN: SLC1 + EXT1	CdPN: 9 + EMER CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: EMER (Unk) CgPN: E164N1 (Nat)
CdPN: 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 220 + 0010 + 4 + 431 + 0001	CdPN: 911 (Unk) CgPN: 212-5550001 (Nat)

IP Phone (with DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- IP Phone (Internal Number: SLC1 + EXT1, with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, "DDI for Emergency" enabled) is making an Emergency call to EMER (Dialed number: EMER)

Figure E-26 IP Phone (with DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: EMER CgPN: SLC1 + EXT1	CdPN: 9 + EMER CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: EMER (Unk) CgPN: E164N1 (Nat)
CdPN: 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 220 + 0010 + 4 + 431 + 0001	CdPN: 911 (Unk) CgPN: 212-5550001 (Nat)

IP Phone (without DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)

- IP Phone (Internal Number: SLC1 + EXT1, without DDI Number) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, "DDI for Emergency" enabled) is making an Emergency call to EMER (Dialed number: EMER)

Figure E-27 IP Phone (without DDI) -> PSTN (Emergency Call, "DDI for Emergency" enabled)

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT'
CdPN: EMER CgPN: SLC1 + EXT1	CdPN: 9 + EMER CgPN: CPID1 + RID1 + CT + SLC1 + EXT1	CdPN: EMER (Unk) CgPN: E164N0 (Nat)
CdPN: 911 CgPN: 431 + 0001	CdPN: 9 + 911 CgPN: 220 + 0010 + 4 + 431 + 0001	CdPN: 911 (Unk) CgPN: 212-5550000 (Nat)

Incoming PSTN Calls

The supported Incoming PSTN calls as follows:

PSTN (National Call) -> IP Phone

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSTN user (E.164 number: PSTN) is making a call to IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1)) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1.

Figure E-28 PSTN (National Call) -> IP Phone

LGW IN	LGW OUT - Unified CM IN	Unified CM OUT
CdPN: E164N1 (Nat) CgPN: PSTN (Nat)	CdPN: CPID1 + RID1 + SLC1 + EXT1 CgPN: PAP1 + NAC1 + PSTN	CdPN: SLC1 + EXT1 CgPN: PAP1 + NAC1 + PSTN
CdPN: 212-5550001 (Nat) CgPN: 214-5551234 (Nat)	CdPN: 220 + 0010 + 431 + 0001 CgPN: 9 + 1 + 214-5551234	CdPN: 431 + 0001 CgPN: 9 + 1 + 214-5551234

PSTN (International Call) -> IP Phone

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSTN user in the UK (E.164 number: E164I5) is making a call to IP Phone (Internal Number: SLC1 + EXT1, DDI Number: E164N1)) in Location 1 on Unified CM cluster 1 in US (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1.

Figure E-29 PSTN (International Call) -> IP Phone

LGW IN	LGW OUT - Unified CM IN	Unified CM OUT
CdPN: E164N1 (Nat) CgPN: E164I5 (Int)	CdPN: CPID1 + RID1 + SLC1 + EXT1 CgPN: PAP1 + IAC1 + E164I5	CdPN: SLC1 + EXT1 CgPN: PAP1 + IAC1 + E164I5
CdPN: 212-5550001 (Nat) CgPN: 44-1632-123456 (Int)	CdPN: 220 + 0010 + 431 + 0001 CgPN: 9 + 011 + 44-1632-123456	CdPN: 431 + 0001 CgPN: 9 + 011 + 44-1632-123456

PSTN (Emergency, CER PSAP Callback) -> IP Phone

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSAP Operator is making a call-back to an Emergency caller (the CgPN delivered to the PSAP operator was ELIN1). The Emergency call was made to EMER from an IP Phone (Internal Number: SLC1 + EXT1, for example with DDI Number: E164N1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1, Cisco ER Configured) IP Phone is in ERL1 (configured with ELIN1, which is associated with CPID1 + RID1 + SLCE + EXTE).

Figure E-30 PSTN (Emergency, CER PSAP CallBack) -> IP Phone

LGW IN	LGW OUT - Unified CM IN	Unified CM OUT
CdPN: ELIN1 (Nat) CgPN: PSAP	CdPN: CPID1 + # + RID1 + SLCE + EXTE CgPN: PAP1 + NAC1 + PSAP	CdPN: 913 + ELIN1 CgPN: PAP1 + NAC1 + PSAP
CdPN: 212-9110000 CgPN: PSAP	CdPN: 220 + # + 0010 + 431 + 0911 CgPN: 9 + 1 + PSAP	CdPN: 913 + 212-9110000 CgPN: 9 + 1 + PSAP
CER IN	**CER OUT - Unified CM IN**	**Unified CM OUT**
CdPN: 913 + ELIN1 CgPN: PAP1 + NAC1 + PSAP	CdPN: SLC1 + EXT1 CgPN: PAP1 + NAC1 + PSAP	CdPN: SLC1 + EXT1 CgPN: PAP1 + NAC1 + PSAP
CdPN: 913 + 212-9110000 CgPN: 9 + 1 + PSAP	CdPN: 431 + 0001 CgPN: 9 + 1 + PSAP	CdPN: 431 + 0001 CgPN: 9 + 1 + PSAP

PSTN (7-digit Local Call, receive NDC) -> IP Phone

In this call scenario:

The CgPN and CdPN is received with the NDC

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSTN User (E.164 number NDC3 + SN4) is making a call to IP Phone (Internal Number: SLC2 + EXT1, DDI Number: NDC3 + SN3) in Location 2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID2)

Figure E-31 PSTN (7-digit Local Call, receive NDC) -> IP Phone

LGW IN	LGW OUT - Unified CM IN	Unified CM OUT
CdPN: NDC3 + SN3 (Sub) CgPN: NDC3 + SN4 (Sub)	CdPN: CPID1 + RID2 + SLC2 + EXT1 CgPN: PAP1 + NDC3 + SN4	CdPN: SLC2 + EXT1 CgPN: PAP1 + NDC3 + SN4
CdPN: 314 + 5550003 (Sub) CgPN: 314 + 5550004 (Sub)	CdPN: 220 + 0100 + 432 + 0001 CgPN: 9 + 314 + 5550004	CdPN: 432 + 0001 CgPN: 9 + 314 + 5550004

PSTN (7-digit Local Call, no NDC) -> IP Phone

In this call scenario:

- The CgPN and CdPN is received without the NDC
- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)

- PSTN User (E.164 number NDC3 + SN4) is making a call to IP Phone (Internal Number: SLC2 + EXT1, DDI Number: NDC3 + SN3) in Location 2 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID2)

Figure E-32 PSTN (7-digit Local Call, no NDC) -> IP Phone

LGW IN	LGW OUT - Unified CM IN	Unified CM OUT
CdPN: SN3 (Sub) CgPN: SN4 (Sub)	CdPN: CPID1 + RID2 + SLC2 + EXT1 CgPN: PAP1 + SN4	CdPN: SLC2 + EXT1 CgPN: PAP1 + SN4
CdPN: 5550003 (Sub) CgPN: 5550004 (Sub)	CdPN: 220 + 0100 + 432 + 0001 CgPN: 9 + 5550004	CdPN: 432 + 0001 CgPN: 9 + 5550004

PSTN (10-digit Local Call) -> IP Phone

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSTN User (E.164 number NDC1 + SN2) is making a call to IP Phone (Internal Number: SLC1 + EXT1, DDI Number: NDC1 + SN1) in Location 1 on Unified CM cluster 1 (PSTN Published Number: E164N0, Unified CM ID: CPID1, Location RID: RID1).

Figure E-33 PSTN (10-digit Local Call) -> IP Phone

Unified CM IN	Unified CM OUT - LGW IN	LGW OUT
CdPN: NDC1 + SN1 (Sub) CgPN: NDC1 + SN2 (Sub)	CdPN: CPID1 + RID1 + SLC1 + EXT1 CgPN: PAP1 + NDC1 + SN2	CdPN: SLC1 + EXT1 CgPN: PAP1 + NDC1 + SN2
CdPN: 212 + 5550001 (Sub) CgPN: 212 + 5550002 (Sub)	CdPN: 220 + 0010 + 431 + 0001 CgPN: 9 + 212 + 5550002	CdPN: 431 + 0001 CgPN: 9 + 212 + 5550002

PSTN -> Voicemail

In this call scenario:

- CdPN NOA is for example set (Yes)
- CgPN NOA is for example set (Yes)
- PSTN user (E.164 number: PSTN) wants to check his Voicemail (Voicemail ID: VMCPID, VoiceMail RID: VMRID, Voicemail Pilot SLC: VMSLC, VoiceMail Pilot Ext: VMEXT, Voicemail DDI Number: E164NVM). The LGW is configured in Location 1 on Unified CM cluster 1 (Unified CM ID: CPID1, Location RID: RID1.

Figure E-34 PSTN -> Voicemail

LGW IN	LGW OUT - Unified CM IN
CdPN: E164NVM (Nat) CgPN: PSTN (Nat)	CdPN: VMCPID + VMRID + VMSLC + VMEXT CgPN: VMCPID + #1# + PAP1 + NAC1 + PSTN
CdPN: 212-5558888 (Nat) CgPN: 212-5551234 (Nat)	CdPN: 300 + 0100 + 200 + 0000 CgPN: 300 + #1# + 9 + 1 + 214-5551234
Unified CM OUT' PGW IN	**PGW OUT ' Movius IN**
CdPN: VMCPID + VMRID + VMSLC + VMEXT	CdPN: VMCPID + VMRID + VMSLC + VMEXT
CgPN: VMCPID + #1# + PAP1 + NAC1 + PSTN	CgPN: PAP1 + NAC1 + PSTN
CdPN: 300 + 0100 + 200 + 0000	CdPN: 300 + 0100 + 200 + 0000
CgPN: 300 + #1# + 9 + 1 + 214-5551234	CgPN: 9 + 1 + 214-5551234

PSTN -> IP Phone -> CF IntraSite -> IP Phone

In this call scenario the first call leg PSTN > IP Phone has already been described in the above sections. For the second call leg (IP Phone -> CF IntraSite -> IP Phone) there is no difference whether the call arrived via Local or Central PSTN access, since the CgPN will be the same and is therefore not covered in this document.

PSTN -> IP Phone -> CF InterSite -> IP Phone

In this call scenario the first call leg (PSTN > IP Phone) has already been described in the above sections. For the second call leg (IP Phone > CF IntraSite > IP Phone) there is no difference whether the call arrived via Local or Central PSTN access, since the CgPN will be the same and is therefore not covered in this document.

The following abbrevations are used in this chapter

Abbrevations	Expansions
CC	Country Code. CC1 (1) - for US and CC2 (44) - for UK, are used in the examples
CPID	Unique Call Processing IDentifier for each Hosted UCS component (Unified CM, PGW, Movius Server, …). CPID1 (220) for Unified CM cluster 1, is used in the example
CT	Call Type.
CT=4	Emergency Call.
CT = 5	Forwarded Call to PSTN.
CT = 6	Forwarded IntraSite or InterSite call (to another location in the same customer.
CT = 8	InterSite call (to another location in the customer).

Abbrevations	Expansions
CT = 9	PSTN call.
E164N	E.164 National number, equal to NDC + SN. E164N0 (212-5550000), E164N07 (314-5550000), E164N1 (212-5550001), E164N2 (646-5550002), E164N3 (314-5550003) and E164N4 (314-5550004) - for the US and E164N5 (1632-123456) are used in the examples.
E164I	E164IE.164 International number for Geographic areas, equal to CC + NDC + SN. E164I0 (1-212-5550000) or (1-314-5550000), E164I1 (1-212-5550001), E164I2 (1-646-5550002), E164I3 (1-314-5550003) and E164I4 (1-314-5550004) - for the US and E164I5 (44-1632-123456) are used in the examples.
ELIN	Emergency Line Identification Number. ELIN1 (212-555911000) is used in the examples.
EMER	Emergency number. EMER (911) is used in the examples.
FREE	Toll-Free Phone Number. FREE (800-NXXXXXX) is used in the examples.
IAC	International Access Code. IAC1 (011) - for the US is used in the examples.
ISP	Customer InterSite Prefix. ISP1 (8) for Customer 1 on Unified CM cluster 1 is used in the examples.
LPS	Location CLIR/CLIP Presentation Setting. LPS1 (restricted) and LPS2 (allowed) are used is used in the examples.
N11	N11 codes, more formally known as service codes, are used to provide three-digit dialing access to special services. N11S (411) is used in the examples.
NAC	National Access Code. NAC1 (1) - for the US is used in the examples.
NDC	National Access Code. NAC1 (1) - for the US is used in the examples.
PAP	Location PSTN Access Prefix. PAP1 (9) for Location 1 on Unified CM cluster 1 is used in the examples.
PREM	Premium Phone Number. PREM (900-NXXXXXX) is used in the examples.
RID	Unique per-"Unified CM cluster" Location Route IDentifier. RID1 (0010) for Location 1 and RID2 (0100) for Location 2 on Unified CM cluster 1 are used in the examples.

Abbrevations	Expansions
SLC	Slate Location Code. SLC1 (431) and SLC2 (432) are used in the examples.
SN	Subscriber Number is a part of the E.164 National (significant) number for Geographic areas. SN0 (5550000), SN1 (5550001), SN2 (5550002), SN3 (5550003) and SN4 (5550004) - for the US and SN5 (123456) - for the UK are used in the examples.

APPENDIX F

Legacy PBX Information

Revised: 08/12/2010, OL-23270-01

This document explains the Leagacy PBX Information for the Hosted UCS Release 7.1(a). The following sections are discussed in this document:

Example IOS Gateway Configuration

Following is an example configuration for a Media Gateway connected to a PBX using PRI QSIG, backhauled to the PGW via MGCP. A 3825 ISR router was used, and the connection to the PBX was made using a VWIC-2MFT-E1-DI Interface Card, in the NM-HDV2-2T1/E1 Network Module:

```
e4qsig#sh ver
Cisco IOS Software, 3800 Software (C3825-IPVOICEK9-M), Version 12.4(15)T3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 24-Jan-08 23:00 by prod_rel_team
```

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

```
e4qsig uptime is 19 weeks, 4 days, 21 hours, 52 minutes
System returned to ROM by power-on
System restarted at 10:34:07 BST Sun Sep 7 2008
System image file is "flash:c3825-ipvoicek9-mz.124-15.T3.bin"
.
.
.
Cisco 3825 (revision 1.2) with 224256K/37888K bytes of memory.
Processor board ID FCZ1139709Z
2 Gigabit Ethernet interfaces
31 Serial interfaces
2 Channelized E1/PRI ports
2 Channelized (E1 or T1)/PRI ports
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
62720K bytes of ATA System CompactFlash (Read/Write)
```

Configuration register is 0x2102

```
e4qsig#sh run
Building configuration...

Current configuration : 2863 bytes
!
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname e4qsig
!
boot-start-marker
boot system flash:c3825-ipvoicek9-mz.124-15.T3.bin
boot-end-marker
!
!card type command needed for slot 1
logging buffered 51200 warnings
enable secret 5 $1$EyO2$rVgOzIpml6Fqo3NMmsy8T0
!
no aaa new-model
clock timezone GMT 0
clock summer-time BST recurring last Sun Mar 2:00 last Sun Oct 3:00
no network-clock-participate slot 1
ip cef
!
!
!
!
no ip domain lookup
ip domain name ipcbuemea.cisco.com
ip host pgw 10.120.4.11 10.121.4.11 10.120.4.12 10.121.4.12
multilink bundle-name authenticated
!
backhaul-session-manager
  set QSIG client ft
  group master set QSIG
  group slave set QSIG
  session group master 10.120.4.11 7007 10.190.4.40 7007 1
  session group slave 10.120.4.12 7007 10.190.4.40 7007 1
  session group master 10.121.4.11 7007 10.191.4.40 7007 2
  session group slave 10.121.4.12 7007 10.191.4.40 7007 2
isdn switch-type primary-qsig
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
!
username cisco privilege 15 secret 5 $1$eLBA$jWOMg6jvjlUXeFW/9g7CC0
!
!
controller E1 1/0/0
 framing NO-CRC4
 pri-group timeslots 1-31 service mgcp
!
controller E1 1/0/1
!
!
!
```

```
!
interface GigabitEthernet0/0
 ip address 10.190.4.40 255.255.255.0
 duplex full
 speed 100
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.191.4.40 255.255.255.0
 duplex full
 speed 100
 media-type rj45
!
interface Serial1/0/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-qsig
 isdn timer T310 120000
 isdn protocol-emulate network
 isdn incoming-voice voice
 isdn bind-l3 backhaul QSIG
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 10.190.4.1
ip route 0.0.0.0 0.0.0.0 10.191.4.1 200
!
!
ip http server
ip http access-class 23
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
!
!
control-plane
!
!
!
voice-port 1/0/0:15
!
!
mgcp
mgcp call-agent pgw 2427 service-type mgcp version 1.0
mgcp dtmf-relay voip codec all mode nse
mgcp max-waiting-delay 1000
mgcp restart-delay 2
mgcp modem passthrough voip mode nse
mgcp codec g711alaw packetization-period 20
mgcp package-capability rtp-package
mgcp package-capability as-package
mgcp default-package gm-package
no mgcp timer receive-rtcp
mgcp bind control source-interface GigabitEthernet0/0
mgcp bind media source-interface GigabitEthernet0/0
!
mgcp profile default
!
!
!
!
!
```

```
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
ntp clock-period 17208472
ntp server 10.100.100.2
ntp server 10.100.100.3
!
end
```

back to Legacy PBX Support (Section 15)

Supported External Node Types on the PGW

To view the External Node Types supported on the PGW, login to the PGW and execute the following:

```
cd /opt/CiscoMGC/etc
more extNodeTypes.dat
```

For example:

PGW-ENT2M% cd /opt/CiscoMGC/etc

PGW-ENT2M% more extNodeTypes.dat

C1751 MGCP IPFAS IUA BRI

C1751_OLD MGCP IPFAS IUA BRI

C1760 MGCP IPFAS IUA BRI

C1760_OLD MGCP IPFAS IUA BRI

C2600 SGCP MGCP IPFAS IUA BRI

C2600_OLD SGCP MGCP IPFAS IUA BRI

C2610XM MGCP IPFAS IUA BRI

C2610XM_OLD MGCP IPFAS IUA BRI

C2611XM MGCP IPFAS IUA BRI

C2611XM_OLD MGCP IPFAS IUA BRI

C2620XM MGCP IPFAS IUA BRI

C2620XM_OLD MGCP IPFAS IUA BRI

C2621XM MGCP IPFAS IUA BRI

C2621XM_OLD MGCP IPFAS IUA BRI

C2650XM MGCP IPFAS IUA BRI

C2650XM_OLD MGCP IPFAS IUA BRI

C2651XM MGCP IPFAS IUA BRI

C2651XM_OLD MGCP IPFAS IUA BRI

C2691 MGCP IPFAS IUA BRI

C2691_OLD MGCP IPFAS IUA BRI

C3600 SGCP MGCP IPFAS NAS IUA

C3640 MGCP IPFAS IUA BRI

C3640A MGCP IPFAS IUA BRI

C3660 SGCP MGCP IPFAS NAS IUA BRI

C3725 MGCP IPFAS IUA BRI

C3725_OLD MGCP IPFAS IUA BRI

C3745 MGCP IPFAS IUA BRI

C3745_OLD MGCP IPFAS IUA BRI

C2801 MGCP IPFAS IUA BRI

C2811 MGCP IPFAS IUA BRI

C2821 MGCP IPFAS IUA BRI

C2851 MGCP IPFAS IUA BRI

C3825 MGCP IPFAS IUA BRI

C3845 MGCP IPFAS IUA BRI

AS5200 IPFAS NAS

AS5300 SGCP MGCP IPFAS NAS IUA MGCPANNO MGCPIVR

AS5350 SGCP MGCP IPFAS NAS BSMV0 IUA MGCPANNO MGCPIVR

AS5400 SGCP MGCP IPFAS NAS BSMV0 IUA MGCPANNO MGCPIVR

AS5800 IPFAS NAS MGCPANNO

AS5850 IPFAS NAS MGCPANNO MGCP IUA MGCPIVR

AS7200 SGCP MGCP IPFAS NAS

CAT8510 MGCP SGCP

CAT8540 MGCP SGCP

MGC EISUP

MGX8260 MGCP IPFAS NAS

MGX8850 MGCP SGCP IPFAS

VISM MGCP SGCP IPFAS

VXSM MGCP SGCP IPFAS IUA H248 MGCPANNO M3UA IPANNO IPTONE CODEC DTMF UDP SCTP

LS1010 MGCP SGCP

SCP	TCAPIP						
TALISS7	SS7SG						
MC3810	MGCP	IPFAS					
SLT	BSMV0						
H323	EISUP						
UNKNOWN	UNKNOWN						
ITP	M3UA SUA						
LIMD	LI						
CCMCLUSTER	N/A						
RACLUSTER	RA						
C7200	H248	DTMF	UDP	TCP	ETSI_NAPT	ITU_IPNAPT	EVPND
C7600	H248	DTMF	UDP	TCP	ETSI_NAPT	ITU_IPNAPT	EVPND
C12000	H248	DTMF	UDP	TCP	ETSI_NAPT	ITU_IPNAPT	EVPND
ASR1000	H248	DTMF	UDP	TCP	ETSI_NAPT	ITU_IPNAPT	EVPND
CRS1	H248	DTMF	UDP	TCP	ETSI_NAPT	ITU_IPNAPT	EVPND

APPENDIX G

Phone Details

Revised: 08/12/2010, OL-23270-01

This document gives the details of Phone Types name and model ID list.

In the table below Column "enum" represents the Product Model ID and "name" represents the "Product Name".

enum	name
30027	Analog Phone
9	Cisco 7935
6	Cisco 7910
7	Cisco 7960
8	Cisco 7940
336	Third-party SIP Device (Basic)
374	Third-party SIP Device (Advanced)
115	Cisco 7941
20000	Cisco 7905
302	Cisco 7985
307	Cisco 7911
308	Cisco 7961G-GE
309	Cisco 7941G-GE
348	Cisco 7931
365	Cisco 7921
369	Cisco 7906
30002	Cisco 7920
30006	Cisco 7970
30007	Cisco 7912
30008	Cisco 7902
30018	Cisco 7961
30019	Cisco 7936

enum	name
404	Cisco 7962
431	Cisco 7937
434	Cisco 7942
435	Cisco 7945
436	Cisco 7965
437	Cisco 7975
540	Cisco 8961
497	Cisco 6961
537	Cisco 9951
495	Cisco 6921
496	Cisco 6941
484	Cisco 7925
493	Cisco 9971

APPENDIX H

Local Gateway Configuration

Revised: 08/12/2010, OL-23270-01

This document provides you the Example Local Gateway Configuration. The following sections are covered in this document.

Local Gateway configuration for PRI port

This section provides you the example running configuration of a local gateway with PRI port (provisioned via USM) for your reference.

```
e1-lgw#sh run
Building configuration...
Current configuration : 8774 bytes
!
! Last configuration change at 13:33:14 UTC Mon Jun 28 2010 by cisco
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname e1-lgw
!
boot-start-marker
boot system flash c2800nm-adventerprisek9_ivs-mz.150-1.M2.bin
boot-end-marker
!
card type e1 0 1
logging buffered 51200 warnings
enable secret 5 $1$sgHJ$Y1SV9774EepM5dot0Zz.k0
enable password cisco
!
no aaa new-model
!
network-clock-participate wic 1
!
dot11 syslog
ip source-route
```

```
!
ip cef
!
no ip domain lookup
ip domain name ipcbuemea.com
no ipv6 cef
!
multilink bundle-name authenticated
!
isdn switch-type primary-net5
!
voice service voip
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 3 g711ulaw
 codec preference 4 g711alaw
!
voice class h323 1
  h225 timeout setup 3
  call start slow
!
voice class h323 8
  h225 timeout tcp establish 2
  call start slow
!
!
!
voice translation-rule 102
 rule 1 /^#1#\(.*\)/ /\1/
!
voice translation-rule 212
 rule 1 /^\(.*\)/ /#1#\1/
!
voice translation-rule 802
 rule 1 /^#2#\(.*\)/ /\1/
!
voice translation-rule 812
 rule 1 /^90900000\(.*\)/ /904\1/
 rule 2 /^90800\(.*\)/ /906800\1/
 rule 3 /^90866\(.*\)/ /906866\1/
 rule 4 /^90877\(.*\)/ /906877\1/
 rule 5 /^90888\(.*\)/ /906888\1/
 rule 6 /^90900\(.*\)/ /907900\1/
 rule 7 /^90700\(.*\)/ /907700\1/
 rule 12 /^900\(.*\)/ /902\1/
 rule 13 /^90\(.*\)/ /901\1/
 rule 14 /^9\(.*\)/ /903\1/
 rule 15 /^8\(.*\)/ /\1/
!
voice translation-rule 911
 rule 1 /^\(.*\)/ /1\1/ type national unknown
 rule 2 /^\(.*\)/ /011\1/ type international unknown
 rule 3 /^1\(.*\)/ /1\1/ type unknown unknown
 rule 4 /^011\(.*\)/ /011\1/ type unknown unknown
 rule 5 /^\(.*\)/ /\1/ type unknown unknown
!
voice translation-rule 912
 rule 1 /^\(.*\)/ /\1/ type national unknown
 rule 2 /^1\(.*\)/ /\1/ type unknown unknown
!
voice translation-rule 9011
 rule 1 /^\(.*\)/ /\1/ type any national
!
```

```
voice translation-rule 9012
 rule 1 /^\(.*\)/ /1\1/ type any unknown
!
voice translation-rule 9021
 rule 1 /^901\(.*\)/ /\1/ type any national
 rule 2 /^902\(.*\)/ /\1/ type any international
 rule 3 /^903\(.*\)/ /\1/ type any unknown
 rule 4 /^904\(.*\)/ /\1/ type any unknown
 rule 5 /^905\(.*\)/ /\1/ type any national
 rule 6 /^906\(.*\)/ /\1/ type any national
 rule 7 /^907\(.*\)/ /\1/ type any national
 rule 8 /^908\(.*\)/ /\1/ type any national
!
voice translation-rule 9022
 rule 1 /^901\(.*\)/ /1\1/ type any unknown
 rule 2 /^902\(.*\)/ /011\1/ type any unknown
 rule 3 /^903\(.*\)/ /\1/ type any unknown
 rule 4 /^904\(.*\)/ /\1/ type any unknown
 rule 5 /^905\(.*\)/ /1\1/ type any unknown
 rule 6 /^906\(.*\)/ /1\1/ type any unknown
 rule 7 /^907\(.*\)/ /1\1/ type any unknown
 rule 8 /^908\(.*\)/ /1\1/ type any unknown
!
voice translation-rule 911305
 rule 1 /^\(.*\)/ /\1/ type subscriber unknown
 rule 2 /^305\(.*\)/ /305\1/ type unknown unknown
!
voice translation-rule 912305
 rule 1 /^\(.*\)/ /305\1/ type subscriber unknown
 rule 2 /^305\(.*\)/ /305\1/ type unknown unknown
!
voice translation-rule 9011305
 rule 1 /^305\(.*\)/ /305\1/ type any subscriber
!
voice translation-rule 9012305
 rule 1 /^305\(.*\)/ /305\1/ type any unknown
!
voice translation-rule 9021305
 rule 1 /^901305\(.*\)/ /305\1/ type any subscriber
!
voice translation-rule 9022305
 rule 1 /^901305\(.*\)/ /305\1/ type any unknown
!
!
voice translation-profile POTSIN21
 translate called 212
!
voice translation-profile POTSIN91
 translate calling 911
 translate called 912
!
voice translation-profile POTSIN91305
 translate calling 911305
 translate called 912305
!
voice translation-profile POTSOUT9011
 translate calling 9011
 translate called 9021
!
voice translation-profile POTSOUT9011305
 translate calling 9011305
 translate called 9021305
!
voice translation-profile POTSOUT9012
```

```
 translate calling 9011
 translate called 9022
!
voice translation-profile POTSOUT9012305
 translate calling 9011305
 translate called 9022305
!
voice translation-profile POTSOUT9021
 translate calling 9012
 translate called 9021
!
voice translation-profile POTSOUT9021305
 translate calling 9012305
 translate called 9021305
!
voice translation-profile POTSOUT9022
 translate calling 9012
 translate called 9022
!
voice translation-profile POTSOUT9022305
 translate calling 9012305
 translate called 9022305
!
voice translation-profile VOIPIN81
 translate called 812
!
voice translation-profile VOIPOUT10
 translate called 102
!
voice translation-profile VOIPOUT80
 translate called 802
!
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
!
application
 service hucsntvoip flash:hucsntvoip.tcl
  param calltype1 9
  param rid1 0010
  param ridlength 4
  param srstmode off
  param emerpubnum1 3053010009
  param rangedigits1 1
  param cpidlength 2
  param emertype1 0
  param gwlocationid 10
  param e164rangestart1 3010000
  param gwfnnid 150
  param natcode1 305
  param rangesize1 10
  param cpid1 01
  param e164rangeprefix1 301000
  param fintrangeprefix1 010010301000
  param pstnpubnum1 3053010000
  param fintrangestart1 0100103010000
 !
 service hucsntpstn flash:hucsntpstn.tcl
  param ridlength 4
  param srstmode off
  param rangedigits1 1
  param cpidlength 2
```

```
  param e164rangestart1 3010000
  param gwfnnid 150
  param pstnaccessprefix1 9
  param natcode1 305
  param countrycode 1
  param rangesize1 10
  param gwelinid 25
  param e164rangeprefix1 301000
  param fintrangestart1 0100103010000
  param fintrangeprefix1 010010301000
  param calltype1 9
 !
!
license udi pid CISCO2821 sn FHK1344F3CL
archive
 log config
  hidekeys
username cisco privilege 15 password 0 cisco
!
redundancy
!
!
controller E1 0/1/0
 framing NO-CRC4
 pri-group timeslots 1-31
 description E1 Controller 0/1/0
!
controller E1 0/1/1
 shutdown
!
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 10.190.1.44 255.255.255.0
 duplex full
 speed 100
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.190.1.44
 !
!
interface GigabitEthernet0/1
 ip address 10.191.1.44 255.255.255.0
 duplex full
 speed 100
 !
!
interface Serial0/1/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn incoming-voice voice
 no cdp enable
 !
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.190.1.1
ip route 0.0.0.0 0.0.0.0 10.191.1.1 200
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
control-plane
```

```
 !
voice-port 0/1/0:15
!
dial-peer voice 11 voip
 translation-profile outgoing VOIPOUT10
 preference 1
 destination-pattern #1#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.3
 voice-class codec 1
 voice-class h323 1
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 81 voip
 translation-profile outgoing VOIPOUT80
 preference 1
 destination-pattern #2#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.3
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 12 voip
 translation-profile outgoing VOIPOUT10
 preference 2
 destination-pattern #1#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.2
 voice-class codec 1
 voice-class h323 1
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 82 voip
 translation-profile outgoing VOIPOUT80
 preference 2
 destination-pattern #2#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.2
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 8 voip
 translation-profile incoming VOIPIN81
 service hucsntvoip
 incoming called-number .
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 91 pots
 translation-profile incoming POTSIN91
 translation-profile outgoing POTSOUT9011
```

```
 preference 1
 service hucsntpstn
 destination-pattern 90[123456789]T
 no digit-strip
 direct-inward-dial
 port 0/1/0:15
 no register e164
!
dial-peer voice 91305 pots
 translation-profile incoming POTSIN91305
 translation-profile outgoing POTSOUT9011305
 preference 1
 service hucsntpstn
 destination-pattern 901305T
 no digit-strip
 direct-inward-dial
 port 0/1/0:15
 no register e164
!
!
gateway
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 login local
line aux 0
 login local
line vty 0 4
 password cisco
 login local
 rotary 1
 transport input telnet
 transport output telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 password cisco
 login local
 transport input telnet
!
scheduler allocate 20000 1000
end
```

Local Gateway configuration for BRI port

This section provides you the example running configuration of a local gateway with BRI port for your reference.

```
e1lgw2#sh run
Building configuration...
Current configuration : 9594 bytes
!
! Last configuration change at 11:42:15 UTC Mon Jun 28 2010 by cisco
!
```

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname e1lgw2
!
boot-start-marker
boot system flash c2800nm-ipvoice_ivs-mz.150-1.M2.bin
boot-end-marker
!
card type e1 0 1
! card type command needed for slot/vwic-slot 1/1
logging buffered 51200 warnings
enable secret 5 $1$SMZ8$Z024T0GrCI0TV1rGL/SJI.
!
no aaa new-model
no network-clock-participate slot 1
network-clock-participate wic 0
network-clock-participate wic 1
!
ip source-route
!
ip cef
!
no ip domain lookup
ip domain name ipcbuemea.cisco.com
no ipv6 cef
multilink bundle-name authenticated
!
isdn switch-type basic-net3
!
voice service voip
 allow-connections h323 to h323
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
 h323
  emptycapability
  h245 passthru tcsnonstd-passthru
 modem passthrough nse codec g711ulaw
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 3 g711ulaw
 codec preference 4 g711alaw
!
voice class h323 1
  h225 timeout setup 3
  call start slow
!
voice class h323 8
  h225 timeout tcp establish 2
  call start slow
!
voice translation-rule 102
 rule 1 /^#1#\(.*\)/ /\1/
!
voice translation-rule 212
 rule 1 /^\(.*\)/ /#1#\1/
!
voice translation-rule 802
 rule 1 /^#2#\(.*\)/ /\1/
!
voice translation-rule 812
 rule 1 /^90900000\(.*\)/ /904\1/
```

```
 rule 2 /^90800\(.*\)/ /906800\1/
 rule 3 /^90866\(.*\)/ /906866\1/
 rule 4 /^90877\(.*\)/ /906877\1/
 rule 5 /^90888\(.*\)/ /906888\1/
 rule 6 /^90900\(.*\)/ /907900\1/
 rule 7 /^90700\(.*\)/ /907700\1/
 rule 12 /^900\(.*\)/ /902\1/
 rule 13 /^90\(.*\)/ /901\1/
 rule 14 /^9\(.*\)/ /903\1/
 rule 15 /^8\(.*\)/ /\1/
!
voice translation-rule 911
 rule 1 /^\(.*\)/ /0\1/ type national unknown
 rule 2 /^\(.*\)/ /00\1/ type international unknown
 rule 3 /^0\(.*\)/ /0\1/ type unknown unknown
 rule 4 /^00\(.*\)/ /00\1/ type unknown unknown
 rule 5 /^\(.*\)/ /\1/ type unknown unknown
!
voice translation-rule 912
 rule 1 /^\(.*\)/ /\1/ type national unknown
 rule 2 /^0\(.*\)/ /\1/ type unknown unknown
!
voice translation-rule 9011
 rule 1 /^\(.*\)/ /\1/ type any national
!
voice translation-rule 9012
 rule 1 /^\(.*\)/ /0\1/ type any unknown
!
voice translation-rule 9021
 rule 1 /^901\(.*\)/ /\1/ type any national
 rule 2 /^902\(.*\)/ /\1/ type any international
 rule 3 /^903\(.*\)/ /\1/ type any unknown
 rule 4 /^904\(.*\)/ /\1/ type any unknown
 rule 5 /^905\(.*\)/ /\1/ type any national
 rule 6 /^906\(.*\)/ /\1/ type any national
 rule 7 /^907\(.*\)/ /\1/ type any national
 rule 8 /^908\(.*\)/ /\1/ type any national
!
voice translation-rule 9022
 rule 1 /^901\(.*\)/ /0\1/ type any unknown
 rule 2 /^902\(.*\)/ /00\1/ type any unknown
 rule 3 /^903\(.*\)/ /\1/ type any unknown
 rule 4 /^904\(.*\)/ /\1/ type any unknown
 rule 5 /^905\(.*\)/ /0\1/ type any unknown
 rule 6 /^906\(.*\)/ /0\1/ type any unknown
 rule 7 /^907\(.*\)/ /0\1/ type any unknown
 rule 8 /^908\(.*\)/ /0\1/ type any unknown
!
voice translation-rule 9111637
 rule 1 /^\(.*\)/ /\1/ type subscriber unknown
 rule 2 /^1637\(.*\)/ /1637\1/ type unknown unknown
!
voice translation-rule 9121637
 rule 1 /^\(.*\)/ /1637\1/ type subscriber unknown
 rule 2 /^1637\(.*\)/ /1637\1/ type unknown unknown
!
voice translation-rule 90111637
 rule 1 /^1637\(.*\)/ /1637\1/ type any subscriber
!
voice translation-rule 90121637
 rule 1 /^1637\(.*\)/ /1637\1/ type any unknown
!
voice translation-rule 90211637
 rule 1 /^9011637\(.*\)/ /1637\1/ type any subscriber
```

```
!
voice translation-rule 90221637
 rule 1 /^9011637\(.*\)/ /1637\1/ type any unknown
!
!
voice translation-profile POTSIN21
 translate called 212
!
voice translation-profile POTSIN91
 translate calling 911
 translate called 912
!
voice translation-profile POTSIN911637
 translate calling 9111637
 translate called 9121637
!
voice translation-profile POTSOUT9011
 translate calling 9011
 translate called 9021
!
voice translation-profile POTSOUT90111637
 translate calling 90111637
 translate called 90211637
!
voice translation-profile POTSOUT9012
 translate calling 9011
 translate called 9022
!
voice translation-profile POTSOUT90121637
 translate calling 90111637
 translate called 90221637
!
voice translation-profile POTSOUT9021
 translate calling 9012
 translate called 9021
!
voice translation-profile POTSOUT90211637
 translate calling 90121637
 translate called 90211637
!
voice translation-profile POTSOUT9022
 translate calling 9012
 translate called 9022
!
voice translation-profile POTSOUT90221637
 translate calling 90121637
 translate called 90221637
!
voice translation-profile VOIPIN81
 translate called 812
!
voice translation-profile VOIPOUT10
 translate called 102
!
voice translation-profile VOIPOUT80
 translate called 802
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice-card 1
 dspfarm
 dsp services dspfarm
```

```
!
!
application
 service hucsntvoip flash:hucsntvoip.tcl
  param calltype1 9
  param rid1 0100
  param srstmode off
  param ridlength 4
  param rangedigits1 1
  param cpidlength 2
  param e164rangestart1 111000
  param gwlocationid 10
  param gwfnnid 150
  param natcode1 1637
  param cpid1 01
  param rangesize1 10
  param e164rangeprefix1 11100
  param fintrangestart1 0101001110000
  param fintrangeprefix1 010100111000
 !
 service hucsntpstn flash:hucsntpstn.tcl
  param srstmode off
  param ridlength 4
  param cpidlength 2
  param rangedigits1 1
  param e164rangeprefix7 6019999
  param natcode4 646
  param fintrangeprefix7 1001006019999
  param elincpid3 10
  param rangesize4 1
  param e164rangestart1 111000
  param gwfnnid 150
  param e164rangeprefix2 6010001
  param fintrangeprefix2 1001006010001
  param pstnaccessprefix1 9
  param rangedigits5 0
  param natcode1 1637
  param countrycode 44
  param calltype9 9
  param e164rangestart5 6010004
  param rangesize1 10
  param calltype4 9
  param gwelinid 25
  param e164rangeprefix1 11100
  param elinslc2 601
  param fintrangestart8 1001006010006
  param fintrangeprefix1 010100111000
  param fintrangestart1 0101001110000
  param calltype1 9
 !
license udi pid CISCO2821 sn FHK1344F3CJ
archive
 log config
  hidekeys
username admin privilege 15 secret 5 $1$aX76$2Ob4W8Mmvwg3riMGX2h3n1
username cisco privilege 15 secret 5 $1$..k5$qj9occu4mQRWvv6bFilHn.
!
!
controller E1 0/1/0
 shutdown
 description E1 port of e2lgw
!
controller E1 0/1/1
!
```

```
interface GigabitEthernet0/0
 ip address 10.190.2.44 255.255.255.0
 duplex full
 speed 100
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.190.2.44
!
interface GigabitEthernet0/1
 ip address 10.191.2.44 255.255.255.0
 duplex full
 speed 100
!
interface BRI0/0/0
 description BRI 0/0/0 - e1lgw2
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn send-alerting
 isdn sending-complete
 isdn outgoing display-ie
 isdn skipsend-idverify
!
interface BRI0/0/1
 no ip address
 isdn switch-type basic-net3
 isdn point-to-point-setup
!
interface BRI1/0/0
 no ip address
 isdn switch-type basic-qsig
 isdn point-to-point-setup
!
interface BRI1/0/1
 no ip address
 isdn switch-type basic-qsig
 isdn point-to-point-setup
!
ip forward-protocol nd
!
no ip http server
ip route 0.0.0.0 0.0.0.0 10.190.2.1
ip route 0.0.0.0 0.0.0.0 10.191.2.1 200
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
control-plane
!
!
voice-port 0/0/0
 cptone GB
!
voice-port 0/0/1
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer voice 11 voip
 translation-profile outgoing VOIPOUT10
 preference 1
 destination-pattern #1#T
 modem passthrough nse codec g711ulaw
```

```
 session target ipv4:10.134.1.3
 voice-class codec 1
 voice-class h323 1
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 81 voip
 translation-profile outgoing VOIPOUT80
 preference 1
 destination-pattern #2#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.3
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 12 voip
 translation-profile outgoing VOIPOUT10
 preference 2
 destination-pattern #1#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.2
 voice-class codec 1
 voice-class h323 1
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 82 voip
 translation-profile outgoing VOIPOUT80
 preference 2
 destination-pattern #2#T
 modem passthrough nse codec g711ulaw
 session target ipv4:10.134.1.2
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 8 voip
 translation-profile incoming VOIPIN81
 service hucsntvoip
 incoming called-number .
 voice-class codec 1
 voice-class h323 8
 dtmf-relay h245-alphanumeric
 fax rate 14400
 no vad
!
dial-peer voice 92 pots
 translation-profile incoming POTSIN91
 translation-profile outgoing POTSOUT9011
 preference 1
 service hucsntpstn
 destination-pattern 90[123456789]T
 no digit-strip
 direct-inward-dial
 port 0/0/0
 no register e164
!
```

```
dial-peer voice 921637 pots
 translation-profile incoming POTSIN911637
 translation-profile outgoing POTSOUT90111637
 preference 1
 service hucsntpstn
 destination-pattern 9011637T
 no digit-strip
 direct-inward-dial
 port 0/0/0
 no register e164
!
gateway
 timer receive-rtp 1200
!
gatekeeper
 shutdown
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 password cisco
 login
 transport input telnet
line vty 5 15
 privilege level 15
 password cisco
 login
 transport input telnet
!
scheduler allocate 20000 1000
end
```