Cisco Hosted Unified Communications Services Release 6.1(a) Provisioning Guide

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-16175-02

Cisco Hosted Unified Communications Services Release 6.1(a) Provisioning Guide

CONTENTS

Preface xxi

Overview xxi

Audience xxi

Organization xxii

Related Documentation xxiii

Obtaining Documentation, Obtaining Support, and Security Guidelines xxiv

Cisco Product Security Overview xxiv

Document Conventions xxv

CHAPTER 1

Hosted UCS Call Routing and Dial Plans 1-1

Overview 1-1

Hosted UCS System Overview 1-2

Numbering 1-3

Dialing Conventions 1-3

Call Routing Between Cisco PGW and Unified CM 1-4

Cisco PGW to Unified CM Interface 1-4

Unified CM to Cisco PGW Call Routing 1-5

Cisco PGW to Unified CM Call Routing 1-6

Example Calls 1-7

Inter-site call (Call Type = 8) 1-7

Call from IP Phone to National PSTN (Call Type = 9) 1-8

Call from PSTN to Unified CM 1-9

Gatekeeper Call Routing 1-10

Cisco H.323 Gatekeepers 1-10
Gatekeeper Routing between Cisco PGW and Cisco Unified CM 1-11
Gatekeeper Routing Between Cisco PGW and Local PSTN Gateways 1-11
Using Dial Plan Models 1-13
Accessing BVSM and Initial Setup 1-14
Accessing the BVSM GUI 1-14
Creating an Internal System Superuser 1-14
Defining Basic Setup Components 1-15
Defining the Dial Plan Type 1-16
Associating the Dial Plan with the Cisco PGW 1-18
Loading the Dial Plan Models 1-18
Loading the Cisco Unified CM Model 1-18
Loading the PGW Model 1-19
Loading the TimesTen Model 1-19

CHAPTER 2 **Defining and Configuring Core Network Elements and Resources** 2-1
Defining Providers and Resources 2-2
Adding Providers 2-2
Managing Number Resources 2-3
Managing Phone Resources 2-4
Managing Services 2-4
Enabling BVSM User Roaming 2-5
Defining and Associating Gatekeepers 2-5
Defining Gatekeepers 2-5
Associating Gatekeepers 2-6
Defining and Associating Cisco PGW 2-7
Defining Cisco PGWs 2-7
Associating Cisco PGWs with a Gatekeeper 2-8
Defining and Configuring Cisco Unified CM Clusters 2-9

Adding Cisco Unified CM Clusters and Publisher Servers 2-9
Adding Cisco Unified Communications Manager Subscriber Servers 2-11
Defining Cisco Unified Communications Manager Groups 2-13
Defining a Cisco Unified Communications Manager Trunk Group in a Cluster 2-14
Importing Softkey Templates 2-15
Viewing Softkey Templates 2-15
Associating Cisco Unified Communications Manager Clusters with Gatekeepers 2-16
Defining and Configuring DHCP Servers 2-16
Adding DHCP Servers 2-17
Loading and Synchronizing DHCP Servers 2-17
Using TFTP Servers 2-18
Defining IP Edge Devices 2-18
Using Music on Hold Servers 2-19
Using Conference Servers 2-19
"Adding Conference Bridges 2-20
Associating Conference Bridges with Cisco Unified CM Clusters 2-21
Configuring Transcoder Servers 2-21
Adding Transcoders 2-22
Associating Transcoders with Cisco Unified CM Clusters 2-23
Adding Cisco PGW-Cisco Unified CM Cluster Hardware Groups 2-23
Loading the Cisco PGW and Cisco Unified CM Clusters 2-24
Loading the Cisco PGW 2-24
Loading Cisco Unified CM Clusters 2-25
Adding Media Resource Groups and Media Resource Group Lists 2-25
Adding Media Resource Groups 2-26
Adding Media Resource Group Lists 2-27
Assigning a Media Resource Group List to Cisco Unified Communications Manager Trunks 2-28

CHAPTER 3 **Managing Countries and Provider Resources** 3-1

Adding Countries 3-2
Adding a Country 3-2
Editing the Incoming Cisco PGW Trunk Group 3-3
Creating an Inventory of E.164 Numbers, IP Addresses, and Phones 3-3
Creating an E.164 Inventory 3-3
Adding Area Codes 3-4
Adding Number Ranges 3-4
Creating an IP Address Inventory 3-5
Creating a Phone Inventory 3-6
Adding Resellers 3-7
Managing Customers 3-8
Adding Customers 3-8
Adding Media Services 3-10
Adding Feature Groups 3-11
Configuring BVSM User Roaming Preferences 3-13
Adding Divisions 3-14
Adding Locations 3-15
Moving Inventory of E.164 Numbers and Phones to Locations 3-18
Moving E.164 Number Inventory 3-19
Moving Phone Inventory 3-20
Administering Locations 3-20
Adding PSTN Published Numbers 3-21
Adding Emergency Published Numbers 3-22
Assigning Range of E.164 Numbers to Internal Numbers 3-23
Assigning Range of E.164 Numbers to Internal Numbers (in-ranges) 3-23
Registering Phones 3-25
Adding an End User 3-26
Adding User Extension Mobility 3-26

Managing Phones 3-28
Managing Users 3-29

CHAPTER 4 **Managing Legacy PBX Support 4-1**

Defining IOS Devices 4-2
Adding IOS Device Types 4-2
Adding IOS Device Network Modules 4-4
Adding IOS Device Interface Cards 4-5
Using Unmanaged PBX Devices 4-6
Adding Unmanaged PBXs 4-6
Adding a Cisco PGW Unmanaged PBX Hardware Group 4-7
Adding Unmanaged PBX Locations 4-8
Adding PSTN Published Numbers 4-10
Adding and Configuring Media Gateways 4-10
Defining Media Gateways 4-10
Configuring Media Gateway Control Protocol 4-11
Configuring Network Modules used on the Media Gateway 4-12
Configuring Interface Cards used on the Media Gateway 4-13
Defining Media Gateway Ports and Trunks 4-13
Associating Media Gateways with the Cisco PGW 4-15
Associating Media Gateways with Unmanaged PBXs 4-15
Creating an E.164 Inventory 4-16
Adding Emergency Published Numbers 4-16
Assigning Range of E.164 Numbers to Internal Numbers 4-17
Assigning Range of E.164 Numbers to Internal Numbers (In-Ranges) 4-17
Understanding Legacy PBX Information 4-19
Viewing a Sample Media Gateway Configuration 4-19
Viewing Supported External Node Types on the Cisco PGW 4-23

CHAPTER 5 **Provisioning Cisco Unified MeetingPlace** 5-1

Overview 5-1

Using MeetingPlace Audio Server 5-5

Understanding LAN Port Details 5-5

Understanding Serial Specifications for Audio Server 5-6

Verifying the Software Release of the Audio Server 5-7

Verifying the Status of the Audio Server Unit 5-8

Configuring the Audio Server System LAN Parameters 5-9

Configuring the Audio Server for Dialing Outbound 5-14

Using MeetingPlace IP Gateway 5-17

Installing the IP Gateway Software 5-17

Setting up the IP Gateway 5-19

Using MeetingPlace Web Conferencing 5-20

Installing the Web Conferencing Server 5-20

MeetingTime Information 5-21

Using MeetingPlace Directory Services 5-22

Licensing MeetingPlace Directory Services 5-22

Installing MeetingPlace Directory Services 5-23

Using MeetingPlace Directory Services Administrator 5-24

Understanding the Interaction with BVSM and LDAP 5-24

Provisioning Cisco Unified Meeting Place 5-25

Provisioning a Cisco Unified MP Hardware Set 5-26

Provisioning the Cisco Unified MP Directory Server 5-26

Provisioning the Cisco Unified MP Directory Service 5-27

Subscribing a Location to the Cisco Unified MP Directory Service 5-27

Creating a Hardware Group for Unified CM 5-28

Provisioning the Cisco Unified MP Conference Service 5-28

CHAPTER 6 **Provisioning Cisco Unity and Movius Voice Messaging Services** 6-1

Provisioning Cisco Unity 6-1

Provisioning Movius Servers 6-4

Using Static Configuration 6-4

Configuring a Virtual IP Address on the Cisco PGW 6-4

Static Cisco PGW Configuration for Movius Servers 6-5

Configuring the Movius Unified Messaging Server 6-5

Configuring Changes to the the Movius Server Model Loader 6-6

Using Network Configuration 6-7

Adding the Movius VoiceMail Server 6-7

Associating the Cisco PGW with other Cisco PGWs 6-8

Associating Unified CM Clusters with other Unified CM Clusters 6-9

Connecting the Movius Server to the Cisco PGW 6-9

Connecting the Unified CM Clusters to the Cisco PGWs 6-9

Configuring Additional Resources 6-10

Creating Voice-Mail Service for Customer 6-11

Allocating the Internal Number for the Voice-Mail Pilot 6-11

Adding the Voice-Mail Service Pilot Number 6-12

Moving the E.164 Number Range for Voice Mail 6-12

Associating the E.164 Number with the Voice Mail Pilot 6-13

Adding the Published Number 6-13

Adding Support for Multiple Classes of Service 6-14

Adding Voice-Mail Service to a Location 6-14

Provisioning Movius AutoAttendant 6-15

Configuring BVSM for Movius AutoAttendant 6-16

Adding AutoAttendant Service 6-17

Adding a Voicemail / AutoAttendant Server 6-17

Adding Voicemail Service for a Customer 6-19

Adding Voicemail Pilot 6-21

Adding a Voicemail Service for a Location 6-24

Creating AutoAttendant Service 6-28
Mapping E164 Number to an AutoAttendant Pilot Number 6-32
Configuring Movius Web Interface for Auto Attendant 6-34
Creating AutoAttendant Service 6-35
Creating Announcements 6-37
Menu Configuration 6-40
AutoAttendant Schedule 6-46
Configuring AutoAttendant Mapping Key 6-47
AutoAttendant Media Termination Point Configuration on Cisco Unified Communications Manager Cluster 6-49

CHAPTER 7 **Provisioning the Local PSTN Breakout Support 7-1**
Introducing Local PSTN Breakout Support 7-1
Handling PSTN Calls via Central Gateway 7-2
Handling PSTN Calls via Local Gateway 7-4
Support for Multiple Trunk Types for Local PSTN Breakout 7-5
Support for Multiple Local Gateway Interfaces 7-5
Support for Cisco Unified SRST 7-6
Provising Local PSTN Breakout Support 7-6
Static Configuration 7-7
Cisco PGW Static Configuration 7-7
Cisco Off-Net HSI Static Configuration 7-10
Cisco Gatekeeper Static Configuration 7-11
Local Gateway Static Configuration 7-11
Loading the IOS Model 7-16
Defining IOS Devices 7-17
Add IOS Device Types 7-17
Add IOS Device Network Modules 7-19
Adding IOS Device Interface Cards 7-20
Initiating Local PSTN Breakout Support 7-21

Adding and Configuring Local Gateways 7-22
Define Local Gateways 7-22
Associate Local Gateways with Gatekeepers 7-23
Configure SRST 7-24
Configure Local Gateway Protocol 7-26
Configure Network Modules used on the Local Gateway 7-26
Configure Interface cards used on the Local Gateway 7-27
Define Local Gateway Interfaces 7-27
Location Administration 7-32
Change Location Preferences 7-32
Connect Locations with Local Gateway Trunk(s) 7-33
Assigning a Range of E164 Numbers to Internal Numbers 7-35

CHAPTER 8 **Provisioning Netwise** 8-1
Netwise Telephony Configuration Application Static Configuration 8-1
Adding a Netwise Cluster to BVSM 8-2
Identifying the Clusters and Servers in BVSM 8-3
Adding a Hardware Group and Console Service to BVSM 8-6
Netwise Server Configuration Performed by BVSM 8-8
CTC 8-8
CMG 8-10
Manual Configuration to Integrate the Netwise Servers 8-11
Configuring CTC 8-11
Configuring Cisco Unified CM 8-13
Configuring Operator Console Attributes 8-13
Configuring Operator Console Attributes 8-14
Adding an Operator Group 8-14
Adding a Console Operator 8-14
CMG Configuration 8-15
Manual Configuration to Add an Operator Console 8-15

Cisco Unified CM 8-15
CTC 8-16
Adding a Pilot Number 8-16
Defining a Pilot Number 8-16
Configuring CTC 8-17
Configuring CMG 8-17
Adding a Console Phone 8-18
Managing Users 8-19
Using Netwise Tools 8-19
Synchronizing Directories 8-20
Synchronizing Netwise Assigned BVSM Locations 8-20
Synchronizing Netwise Assigned Console Operators 8-21
Releasing all Console Services from a Location 8-21
Releasing all Console Operators for a Location 8-21
Destroying a Location 8-22
Standard Parameter Fields and Standard Layout 8-22
Standard Parameter Fields 8-22
Standard Layout 8-23

CHAPTER 9 **Provisioning NAT/PAT Support 9-1**
Support for NAT/PAT 9-1
Support for NAT/PAT Through Autoregistration of IP Phones 9-2
Supported Scenarios for DHCP Services 9-2
How IP Phone Autoregistration Provides NAT/PAT Support 9-3
Limitations in Support for NAT/PAT 9-4
Provisioning Unified CM to Support NAT/PAT 9-4
Auto-registration 9-5
Configuring Auto-registration 9-5
Provisioning BVSM to Support NAT/PAT 9-9

Configuring BVSM Webmin 9-10
Configuring DHCP Services on an External Server 9-14
BVSM DHCP Configuration 9-15
BVSM Provider Configuration 9-16
BVSM Customer Configuration 9-18
BVSM Location Administration 9-21

CHAPTER 10 **Provisioning Shared Building** 10-1

Building Administration 10-1
Adding a Building 10-2
Add Site Codes 10-5
Add Building Voicemail Service 10-6
Selecting VoiceMail Service Profile 10-7
Add AutoAttendant Service 10-7
Adding and Moving E164 Numbers to VoiceMail Service for the VoiceMail and AutoAttendant Service Pilot Numbers 10-8
Add Feature Groups 10-9
Adding Customer, Division, and Shared Building Location Including VoiceMail and AutoAttendant Services 10-10
Moving Inventory of E164 Numbers and Phones to Shared Building Locations 10-13
Move E164 Number Inventory 10-14
Move Phone Inventory 10-15
Building Location Administration 10-15
Adding PSTN Published Number 10-16
Adding Emergency Published Number 10-17
Assigning Range of E164 Numbers to Internal Numbers 10-18
Registering Phones 10-19
Adding End User 10-20
Adding User Extension Mobility 10-21

Adding User Roaming (Cross Cluster Forwarding) 10-22
Managing Phones 10-24
Managing User 10-24

CHAPTER 11 **Provisioning Cisco Emergency Responder** 11-1
Cisco Emergency Responder Integration 11-2
Planning for Cisco Emergency Responder Integration 11-2
Routing Emergency Calls in Hosted UCS without Cisco Emergency Responder 11-3
Routing Emergency Calls in Hosted UCS with Cisco Emergency Responder 11-6
Provisioning Cisco Emergency Responder Integration 11-17
Static Configuration 11-17
Cisco Emergency Responder Static Configuration 11-17
LAN Switch Static Configuration 11-20
Cisco Unified Communications Manager Static Configuration 11-20
Provisioning Cisco Emergency Responder Support 11-22
Adding and Configuring Cisco ER Groups 11-22
Adding Locations with Enhanced Emeergency Support 11-31
Location Administration 11-32

CHAPTER 12 **Provisioning Cisco Unified Contact Center Hosted Integration** 12-1
Provisioning Cisco Unified Contact Center Hosted feature 12-2
Configuring CUCM Application User and PG User 12-2
Adding and Configuring Cisco CVP and VXML gateway 12-2
Adding Contact Center pilot numbers (pre-routing calls) 12-5
Contact Center Agents Administration 12-7
Provisioning HUCS for additional options (Post-routing calls, Cisco IP IVR) 12-12
Static/manual Configuration 12-14

Configuring CUCM Application User and PG User 12-15
Configuring Application User in CUCM 12-15
Configuring PG User in Peripheral Gateway 12-16
Configure CVP and VXML gateway for HUCS 12-17
Configuring CVP for HUCS 12-17
Configuring VXML gateway for HUCS 12-18
Associate phone to application user 12-25
Create route-point and associated DNs (post-routing calls) 12-25
Create CTI route points 12-26
Associate DN (lines) to the CTI route point 12-27
Associate CTI route points to Application User 12-27
Create CTI ports and associated DNs (Cisco IP IVR) 12-28
Create Application User 12-28
Create CTI ports and associated DNs for every customer IP IVR 12-28
Create CTI route points (IVR triggers) and associated DNs for every customer IP IVR 12-30

CHAPTER 13 **Provisioning Other Hosted Unified Communications Services Features** 13-1

Provider Specific Features 13-2
Forced Central PSTN Breakout 13-2
Forced To Use 13-2
Allowed To Use 13-3
Forced OffNet 13-4
Customer Specific Features 13-5
Enable BO2OT on Unified CM 13-6
Configure BO2OT for Specific Customers 13-7
Configure BO2OT for Customers in a Building 13-8
Location Specific Features 13-8
NPA Overlay 13-9
NPA Geographic Split 13-9

Phone Specific Features 13-11
Create Service Type for the XML Phone Service 13-11
Add XML Phone Service to a Feature Group 13-12
Personalize phone with XML Application 13-12

APPENDIX A **Hosted Unified Communications Services Location Administration A-1**
User Interface Guidelines A-1
Quick Search A-2
Phone Management A-4
Transactions (General Tools) A-6
Hunt Groups A-6
Managing Hunt Groups A-7
Managing Lines in a Hunt Group A-8
Line Groups A-10
Creating a Line Group A-10
Adding a Line to a Line Group A-12
Pickup Groups A-12
Adding Numbers to a Pickup Group A-12
Associating Pickup Groups A-15
Users A-16
Managing User Accounts A-16
Adding a User Account A-17
Managing Voice Mail Accounts A-20
Managing Mobility Profiles A-21
Associating and Unassociating a Phone with a User A-22
Deleting a User Account A-24
Phone Registration A-24
Phone Management A-26
Extensions A-28

A-29

APPENDIX B **Hosted Unified Communications Services Division Administration** B-1

Overview B-1

User Interface Guidelines B-1

Quick Search B-2

Managing Phones B-4

Phone Management Summary B-4

Manually Adding Phones B-5

Removing Phones B-5

Managing Internal and External Numbers B-6

Managing Services B-6

Resources/Phone Inventory B-7

General Tools B-10

Transactions B-10

Basic Reports B-11

General Administration B-13

Locations B-13

Adding a Location B-14

Managing Location Resources B-16

PSTN Published Number B-17

Internal Published Number B-18

Emergency Number B-19

VoiceMail Management B-20

Location Administration B-22

Hunt Groups B-23

Using a Hunt Group with Multiple Number Groups B-25

Number Groups B-25

Voicemail Groups B-25

Pickup Groups B-27
Users B-28
Phone Registration B-31
Phone Management B-32
Internal Numbers B-32

APPENDIX C **Hosted Unified Communications Services Customer Administration C-1**

Overview C-1
User Interface Guidelines C-2
Quick Search C-2
Provisioning Guidelines C-4
Managing Phones C-5
Phone Management Summary C-5
Manually Adding Phones C-5
Removing Phones C-6
Autoprovisioning C-6
Managing Internal and External Numbers C-8
Managing Services C-9
Using the Pilot Number C-10
Setup Tools C-10
Samples C-11
Developer Tools C-11
Tutorials C-12
Provider Administration/Feature Templates C-13
Resources/Phone Inventory C-15
General Tools C-18
Deployment Tools C-18
Transactions C-19
Basic Reports C-20

General Administration C-22
Users C-22
Divisions C-23
Tenants C-26
Locations C-27
Adding a Location C-28
Managing Location Resources C-31
PSTN Published Number C-32
Internal Published Number C-33
Emergency Number C-34
VoiceMail Management C-35
Feature Groups C-37
Location Administration C-40
Switchboards C-40
Telephony C-42
Hunt Groups C-44
Using a Hunt Group with Multiple Line Groups C-47
Number Groups C-47
Voicemail Groups C-48
Pickup Groups C-49
Users C-50
Phone Inventory C-53
Phone Registration C-54
Phone Management C-55
Analogue Line Reg. C-56
Analogue Line Mgt. C-56
MoH Track Mgt Option C-57
Internal Numbers C-59
Internal Numbers C-59
External Numbers C-60

Data Services C-62

Preface

This preface includes the following sections:

- Overview, page xxi
- Audience, page xxi
- Organization, page xxii
- Related Documentation, page xxiii
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xxiv
- Document Conventions, page xxv

Overview

This guide describes how to use Vision OSS BVSM 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 6.1(a).

This document is to be used with the documentation for the individual components of the Hosted UCS 6.1(a) platform after completing the high-level design (HLD)D 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 in a Hosted UCS system, and explains how dial plans are used and loaded to the system.
Chapter 2, “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 3, “Managing Countries and Provider Resources”	Describes how to define and configure other BVMS objects and resources, such as countries.
Chapter 4, “Managing Legacy PBX Support”	Describes how to integrate the Hosted Unified Communications Services platform with legacy PBX systems.
Chapter 5, “Provisioning Cisco Unified MeetingPlace”	Describes how to provision the Hosted Unified Communications Services platform for use with Cisco Unified MeetingPlace.
Chapter 6, “Provisioning Cisco Unity and Movius Voice Messaging Services”	Describes how to provision the Hosted Unified Communications Services platform for use with Cisco Unity Messaging and Mereon IP Unity Messaging systems.
Chapter 7, “Enhancements to the Hosted UCS Dial Plan”	Describes how to provision the North American Dial Plan and dial plans for countries without area codes.
Chapter 8, “Provisioning Netwise”	Describes how to provision the Hosted Unified Communications Services platform for use with Netwise.

Chapter 9, “Provisioning NAT/PAT Support”	Describes how to configure Cisco Hosted UCS components when IP phones are connected to the BVSM server through a Cisco NAT/PAT device.
Chapter 10, “Provisioning Shared Building”	Describes the steps required to configure the Shared Building feature introduced with Cisco Hosted Unified Communications Services, Release 6.1(a).
Chapter 11, “Provisioning Cisco Emergency Responder”	Describes enhanced emergency call routing using Cisco Emergency Responder (Cisco ER) via local gateways in the Hosted UCS reference architecture for Hosted Uunified Communications Services 6.1(a)
Chapter 12, “Provisioning Cisco Unified Contact Center Hosted Integration”	Describes the required steps to configure the Cisco Unified Contact Center Hosted (UCCH) Integration feature introduced with Cisco Hosted Unified Communications Services (UCS), Release 6.1(a).
Chapter 13, “Provisioning Other Hosted Unified Communications Services Features”	Describes how to use VisionOSS Business Voice Services Manager (BVSM) application to provision the components of the Cisco Hosted Unified Communications Services (HUCS), Release 6.1(a) platform.

Related Documentation

For more information, see the following guides:

- *Release Notes for Cisco Hosted Unified Communications Services (Hosted UCS), Release 6.1(a), Maintenance Release 1*

  http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/61_a/english/release/mr1/hucrn51b_mr1.pdf

- *Software Support Matrix for Cisco Hosted Unified Communications Services (Hosted UCS), Release 6.1(a)*

  http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/61_a/english/software_matrix/softwarematrix_61a.pdf

- *Getting Started with Cisco Hosted Unified Communications Services, Release 6.1(a)*

  http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/61a/english/user/gettingstarted_61a.pdf

- *Solutions Reference Network Design for Cisco Hosted Unified Communications Services (Hosted UCS), Release 6.1(a)*

  To obtain a copy of the Solution Reference Network Design document for Cisco Hosted Unified Communications Services, Release 6.1(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:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	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.
< >	Nonprinting characters, such as passwords are in angle brackets.

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) 6.1(a) deployment. It also describes how to use the Vision OSS Business Voice Services Manager (BVSM) application to load dial plan models. This section includes the following sections:

- Overview, page 1-1
- Call Routing Between Cisco PGW and Unified CM, page 1-4
- Gatekeeper Call Routing, page 1-10
- Using Dial Plan Models, page 1-13

Overview

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

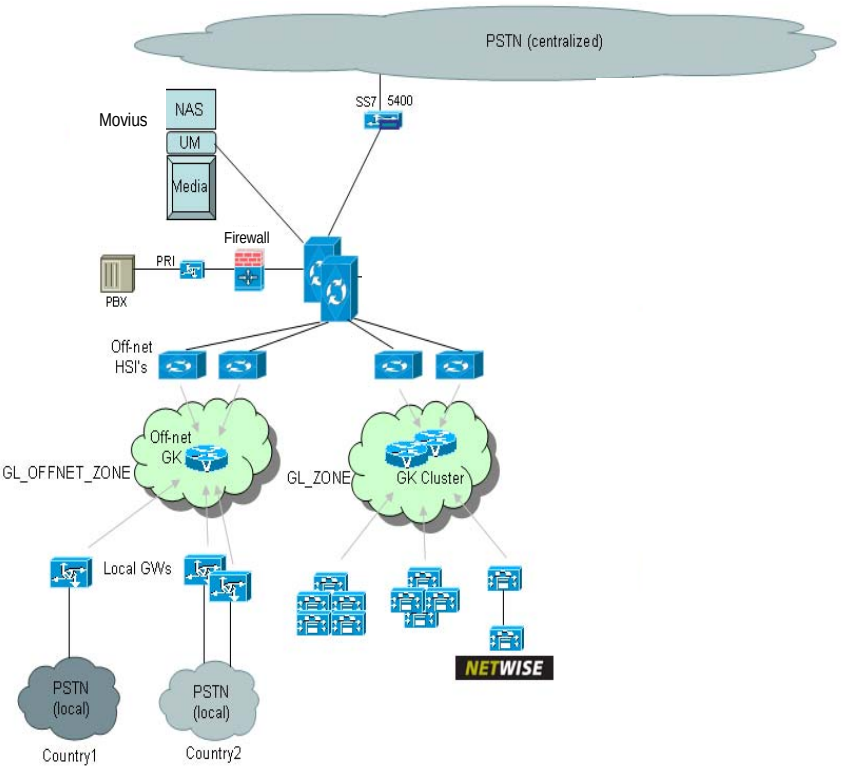
- Hosted UCS System Overview, page 1-2
- Numbering, page 1-3
- Dialing Conventions, page 1-3

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. BVSM 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.

BVSM 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 VisionOSS BVSM, 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 BVSM
- RID (Routing ID): A value for a Location, unique per CPID, which is dynamically allocated by BVSM
- 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

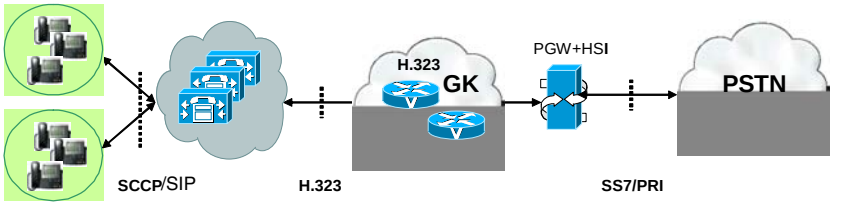
This section describes how call routing occurs between the Cisco PGW and a Unified CM cluster. It includes the following topics:

- Cisco PGW to Unified CM Interface, page 1-4
- Unified CM to Cisco PGW Call Routing, page 1-5
- Cisco PGW to Unified CM Call Routing, page 1-6
- Example Calls, page 1-7

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.

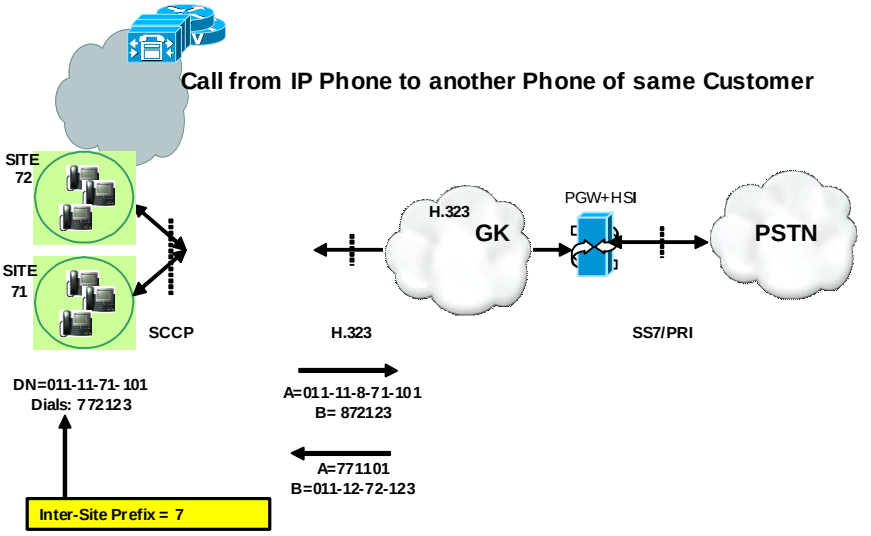
Inter-site call (Call Type = 8)

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

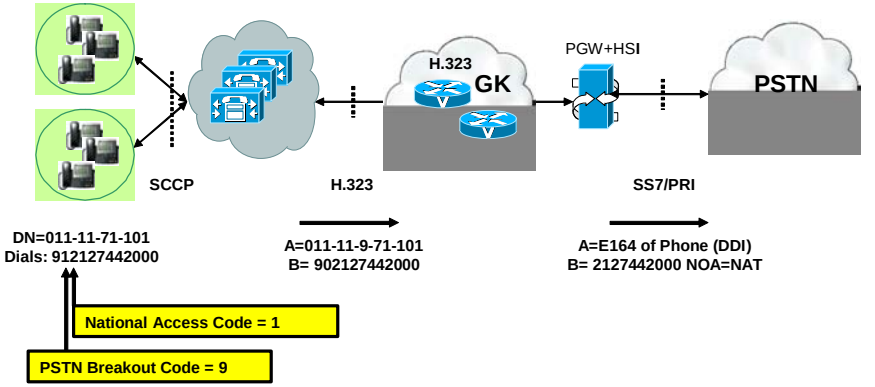


Call from IP Phone to National PSTN (Call Type = 9)

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.

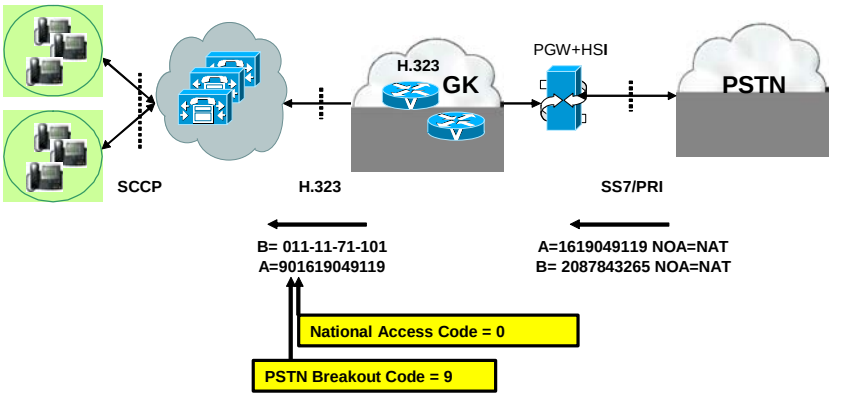
Figure 1-4 Numbering on interface between Unified CM and the Cisco PGW for a National PSTN Call in US



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, page 1-10
- Gatekeeper Routing between Cisco PGW and Cisco Unified CM, page 1-11
- Gatekeeper Routing Between Cisco PGW and Local PSTN Gateways, page 1-11

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 BVSM 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 BVSM 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#.

Gatekeeper Routing Between Cisco PGW and Local PSTN Gateways

Use of local PSTN gateways is an optional feature in Hosted UCS. If it is required in a deployment, then the H.323 zone, HUCS_OFFNET_ZONE, is used for routing calls between the Cisco PGW and the local gateways. A pool of Cisco HSI

dedicated to Cisco PGW-to-local gateway calls and the local gateway will register within this zone. The two types of HSI (On-net and Offnet) may register to the same gatekeeper device. However, because they register in different zones, they are always considered entirely separate from a call routing perspective. The Cisco PGW uses the ILGW dialplan for handling calls received from the Offnet HSI along with the dedicated route list *rltist2offnethsi* to send calls through the Offnet HSI to local gateways.

Call routing within this zone is based entirely on the technology-prefix, and no inter-zone call routing is used.

The Cisco local gateways are IOS H.323 devices which will be automatically configured by BVSM to register with the gatekeeper zone HUCS_OFFNET_ZONE using a gateway identifier as the technology prefix. Because the Cisco PGW sends calls to a local gateway via the gatekeeper with a called number beginning with the gateway identifier, calls are routed to the correct PSTN gateway. The gatekeeper simply analyses the called number matching its leading digits to the gateway identifier of registered local gateways.

The Offnet HSI must register with a technology prefix of 999#, which must also be configured as the default technology prefix on the gatekeeper. This means that any call that does not start with a valid gateway identifier will automatically be sent to the Offnet HSI for handling by the Cisco PGW. This is intended for calls received from the PSTN via the local gateways.

Inbound calls from the PSTN (via the local gateways) will never start with a gateway identifier (which always includes ‘#’) so these calls will be handled by this default call routing. The Cisco PGW must always prefix a gateway identifier to outbound calls (towards the local gateways) so that the gatekeeper routes based on this prefix. No gateway may use a gateway identifier matching the default technology-prefix 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:

- Accessing BVSM and Initial Setup, page 1-14
- Defining the Dial Plan Type, page 1-16
- Associating the Dial Plan with the Cisco PGW, page 1-18
- Loading the Dial Plan Models, page 1-18

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 BVSM database. Models are created using Microsoft Excel files and BVSM loads the configuration by importing the Excel files. Importing these spreadsheets updates the BVSM database but does not actually provision the components. The data in the models is in the form of templates that are used by BVSM 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 BVSM using different BVSM bulk load tools. BVSM stipulates that the first sheet in the file must be a Version sheet which is used to ensure the model data is compatible with the BVSM software version.

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

Accessing BVSM and Initial Setup

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

- Accessing the BVSM GUI, page 1-14
- Creating an Internal System Superuser, page 1-14
- Defining Basic Setup Components, page 1-15

Accessing the BVSM GUI

To access the BVSM GUI, perform the following steps:

Procedure

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

Step 2 Log in as the superuser **bvsm**:

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

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

Step 3 Change the password of the superuser **bvsm** to an appropriate strong password.

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*>

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 BVSM 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 BVSM by loading the raw API commands (BVSMAPI worksheet), perform the following steps:

Procedure

Step 1 Choose **General Tools > Deployment Tools**.

Step 2 Click **Base Data**.

Step 3 Browse for the model loader being used and click **Upload file**.

This loads the information from the BVSMAPI worksheet into the BVSM database, including the following:

- Standard Cisco Unified CM phone button templates
- Standard Cisco Unified CM phone types
- Service types, which are used in the Cisco Unified CM model for defining class of service (CoS) configuration. This is customer-specific.

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

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

This section includes the following topics:

- Defining the Dial Plan Type, page 1-16
- Associating the Dial Plan with the Cisco PGW, page 1-18

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—**MT**
- Description—**Hosted UCS 6.1(a) Multi-Tenant 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.

Loading the Dial Plan Models

This section describes the steps for loading the core Hosted UCS 6.1(a) models (Cisco PGW and Cisco Unified CM). The models define how BVSM should configure the Cisco PGW and Cisco Unified CM. This section includes the following topics:

- Loading the Cisco Unified CM Model, page 1-18
- Loading the PGW Model, page 1-19
- Loading the TimesTen Model, page 1-19

Loading the Cisco Unified CM Model

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

Procedure

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

Step 2 Click **Load Unified CM Models**.

Step 3 Browse for the model loader being used and click **Upload file**.

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

Loading the PGW Model

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

Caution When Loading the PGW Model in BVSM, BVSM also tries to load the PGW_TimesTen_Any worksheet. Bugzilla 3753 has been opened to address this issue.

Procedure

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

Step 2 Click **Load PGW Models**.

Step 3 Browse for the model loader being used and click **Upload file**.

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

Loading the TimesTen Model

To prepare BVSM by loading the 'PGW_TimesTen_Any' PGW TimesTen Model, perform the followinf steps:

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

Step 2 Click **Load TimesTen model statements**.

Step 3 Browse for the model loader being used and click **Upload file**.

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

CHAPTER 2

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:

- Defining Providers and Resources, page 2-2
- Defining and Associating Gatekeepers, page 2-5
- Defining and Associating Cisco PGW, page 2-7
- Defining and Configuring Cisco Unified CM Clusters, page 2-9
- Defining and Configuring DHCP Servers, page 2-16
- Using TFTP Servers, page 2-18
- Defining IP Edge Devices, page 2-18
- Using Music on Hold Servers, page 2-19
- Using Conference Servers, page 2-19
- Configuring Transcoder Servers, page 2-21
- Adding Cisco PGW-Cisco Unified CM Cluster Hardware Groups, page 2-23
- Loading the Cisco PGW and Cisco Unified CM Clusters, page 2-24
- Adding Media Resource Groups and Media Resource Group Lists, page 2-25

Defining Providers and Resources

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:

- Adding Providers, page 2-2
- Managing Number Resources, page 2-3
- Managing Phone Resources, page 2-4
- Managing Services, page 2-4

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—**PGW-Unified CM:MT**

Step 5 From the GUI Branding menu, define the type of branding required.

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

Step 6 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
- Internal Extensions
- Analog PSTN Lines
- Incoming Lines
- Outgoing Lines
- Emergency Call Back Lines

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, music on hold, 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 BVSM User Roaming

To enable the option to use BVSM 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 BVSM as a Cisco 36xx Series Router.

Note Starting with Hosted UCS 5.1(b), gatekeepers are supported on various router types, not only on 36xx Series Routers.

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-ENT3A**
- IP Address—<*gatekeeperIP*>; for example, **10.120.3.51**
- Description—<*gatekeeperdescription*>; for example, **City 3 Gatekeeper A**
- Config Password—<*configpassword*>; for example, **cisco**
- Enable Password—<*enablepassword*>; for example, **cisco**
- Version—<*gatekeeperIOSversion*>; for example, **Cisco36xx: 12.3**

Note In Hosted UCS 6.1(a), the required Cisco IOS version for gatekeepers is 12.4(11)T3. Therefore, there should be an option to choose the 12.4 IOS version.

Step 5 Click **Add**.

Repeat this procedure for all gatekeepers.

Associating Gatekeepers

This is an optional step that applies 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 BVSM 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-ENT3**
- Description—<*pgwdescription*>; for example, **City 3 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-ENT3M**
- Primary IP Address—<*primaryIP*>; for example, **10.120.3.11**
- Secondary IP Address—<*secondaryIP*>; for example, **10.121.3.11**
- Config Username—<*configusername*>; for example, **mgcusr**
- Config Password—<*configpassword*>; for example, **cisco**
- Config Prompt—**%**
- MML command—**mml –s8**
- Congestion threshold—specify the tolerance for congestion in your deployment
- 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-ENT4M**
- Primary IP Address—<*primaryIP*>; for example, **10.120.4.11**
- Secondary IP Address—<*secondaryIP*>; for example, **10.121.4.11**
- 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 7 Click **Add**.

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:

1. Add Cisco Unified CM clusters and publisher servers
2. Add Cisco Unified CM subscriber servers
3. Define Cisco Unified CM groups
4. Import Softkey Templates
5. Associate Cisco Unified CM cluster with gatekeepers

Adding Cisco Unified CM Clusters and Publisher Servers

Cisco Unified CM is defined in BVSM 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 Unified CM.

Step 4 From the Unified CM Cluster Details menu, enter the following:

- Software Version—<*UnifiedCMVersion*>, for example, **CCM : 4.2.0**
- Name—<*uniquename*>; for example, **e3c1**
- Description—<*cucmclusterdescript*>; for example, **City 3 cluster 1 4.2(3)sr3**
- Publisher Host Name—<*publisheripaddress*>; for example, **10.131.3.2**
- 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.

Note Bugzilla 3024 has been opened to address the issue of the length of this field being limited to 11 characters, and for using Wins Hostname (which does not exist in 5.x). For more information, see the following URL: https://visionoss.eu/bugzilla/show_bug.cgi?id=3024

- Publisher IP Address—<*publisheripaddress*>; for example, **10.131.3.2**
- 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**
- Publisher Config Password—<*publisherpassword*>
- 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**
- 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, **30000**
- 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, **10.131.3.3**
- Wins Hostname—<*shorthostname*>; for example, **e3c1s1**.

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

Note Bugzilla 3024 has been opened to address the issue of the length of this field being limited to 11 characters, and for using Wins Hostname (which does not exist in 5.x). See: https://visionoss.biz/bugzilla/show_bug.cgi?id=3024

- Unified CM Name—<*shorthostname*>; for example, **e3c1p**
- Description—<*subscriberdescript*>; for example, **City 3 cluster 1 4.2(3)sr3 Subscriber 1**
- IP Address—<*subscriberipaddress*>; for example, **10.131.3.3**
- 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**

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, **e3PhoneGroupClu1**
- Description—<*phonegroupdesc*>; for example, **Phone Group in City 3 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:
  - **e3c1p** (Publisher)
  - **e3c1s1** (Subscriber 1 Local)
  - **esc2s2** (Subscriber 2 - Remote)
  - **e3c1s3** (Subscriber 3 - Local)
- Set the server order for the selected servers; for example:

  - Server Order—**0- e3c1s1**
  - Server Order—**1- e3c2s2**
  - Server Order—**2- e3c1s3**
  - Server Order—**3- e3c1p**

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 trunk group.

Step 3 Click **Groups**.

Step 4 Click **Add**.

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

- Group Name—<*trunkgroupname*>; for example, **e3TrunkGroupClu1**
- Description—<*trunkgroupdesc*>; for example, **Trunk Group in City 3 Cluster 1**
- Maximum Streams Supported—<*maxstreams*>; for example, **10000**
- Click **Use for Trunks**.

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

- Choose all servers that are in the list; for example:
  - **e3c1p** (Publisher)
  - **e3c1s1** (Subscriber 1 - Local)
  - **esc2s2** (Subscriber 2 - Remote)
  - **e3c1s3** (Subscriber 3 - Local)

- Set the server order for the selected servers; for example:
  - Server Order—0- **e3c1s1**
  - Server Order—1- **e3c2s2**
  - Server Order—2- **e3c1s3**
  - Server Order—3- **e3c1p**

Step 7 Click **Submit**.

Repeat this procedure for all Cisco Unified CM clusters.

Importing Softkey Templates

To import the softkey templated 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**.

Step 5 Click **Import**.

Viewing Softkey Templates

To view the imported Softkey 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**.

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.

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 BVSM 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-ENT3**
- IP Address—<*bvsmvirtualIP*>; for example, **10.120.3.62**
- Description—<*dhcpserverdescription*>; for example, **City 3 DHCP server on BVSM**
- Config User Name—**dhcp**
- Config Password—Leave the default password
- Path and name of config file—**/data/extdhcp/etc/dhcp/dhcpd.conf**
- Path and name of leases file—**/data/extdhcp/var/lib/dhcp/dhcpd.leases**
- Version—**ISC: 3.0.X**

Step 5 Click **Add**.

Repeat this procedure for all DHCP servers.

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.conf file 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, you 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 TFTP servers can also be added as an IOS Device or Technician.

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 BVSM 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, **e3clu1cus1loc2IPEdge**
- IP Address—<*ipedgeIP*>; for example, **10.181.3.65** (this is the IP helper address for the phones in City 3 - cluster1 customer 1 location 2)
- Email Address: <*email*>; for example, **admin112@company1.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 Music servers can also be added as a Technician.

Using Conference Servers

The conference server is defined in BVSM as a Technician or CiscoMPDirectory.

The CiscoMPDirectory product is used to provision the MeetingPlace server.

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

Note These are optional steps, and are only required for testing conferencing. Also note that the Unified CM Conference Bridge Software is defined in BVSM if the Conference Server checkbox was selected during the Publisher and/or Subscriber configuration.

"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, **C0700192FD31FE43**
- IP Address—<*conferenceIP*>, IP address of the conference bridge device or Cisco Unified CM server (for software conference bridges); for example, **10.181.3.65**
- 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 BVSM 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 BVSM 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, **e4-xcode1**
- IP Address—<*xcodeIP*>, the IP address of the transcoder device; for example, **10.190.3.111**
- 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 BVSM 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

BVSM 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, **e3pgwcucmhwgrpclu1**

- Description—<*hwgrpdesc*>; for example, **City 3 PGW-CUCM Hardware Group Cluster 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-ENT3**.

Step 5 From the Available PBX Systems menu, choose the required Cisco Unified CM cluster; for example, **e3c1**.

Repeat this procedure for all Cisco Unified CM clusters.

Note For BVSM 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, BVSM 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 BVSM 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**.

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, **e3mrgClu1**
- Description—<*mrgdescript*>; for example, **Media Resource Group in City 3 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**.

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

This procedure updates both BVSM 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, **e3mrglClu1**
- Description—<*mrgldescript*>; for example, **Media Resource Group List in City 3 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 BVSM 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, **e3c1-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 BVSM 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.

CHAPTER 3

Managing Countries and Provider Resources

This chapter describes how to use BVSM 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, page 3-2
- Creating an Inventory of E.164 Numbers, IP Addresses, and Phones, page 3-3
- Adding Resellers, page 3-7
- Managing Customers, page 3-8
- Adding Divisions, page 3-14
- Adding Locations, page 3-15
- Moving Inventory of E.164 Numbers and Phones to Locations, page 3-18
- Administering Locations, page 3-20

Note This document describes the provisioning instructions required to implement a basic Hosted UCS solution. For detailed instructions regarding the different optional features, refer to the VisionOSS BVSM documentation.

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, page 3-2
- Editing the Incoming Cisco PGW Trunk Group, page 3-3

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 BVSM, 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 Separate DHCP servers are required to add another country to the same BVSM server.

Editing the Incoming Cisco PGW Trunk Group

As part of Hosted UCS 6.1(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 3-3
- Creating an IP Address Inventory, page 3-5
- Creating a Phone Inventory, page 3-6

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 > E164 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, **1631**.

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, **1631**, 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, **10.181.4.64**
- Subnet Mask—<*subnetmask*>; for example, **/26**
- DHCP server controlling this subnet—<*dhcpserver*>; for example, **dept1-ftp**
- IP edge device to which this subnet is connected—<*ipedge*>; for example, **myedgedevice**
- Origin IP of DHCP messages encapsulated by router—<*defaultip*>; for example, **10.181.4.65**
- DHCP helper IP address—<*bvsmvirtualIP*>; for example, **10.120.3.62**
- Backup DHCP helper IP address—<*bvsmvirtualIP*>; for example, **10.120.3.62**
- Domain Name—<*domainname*>; for example, **dept1.mydomain.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, **10.181.4.65**

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 From BVSM version 3.1.8 alpha 11, it is possible to assign a non-default phone button template to an IP phone. 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 3-1:

Figure 3-1 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**.

You can also configure non-default 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.

You define which Hosted UCS network components are associated with the customer by selecting an appropriate hardware group. In addition, the dialing prefix used for calls between customer locations is defined 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 3-8
- Adding Media Services, page 3-10
- Adding Feature Groups, page 3-11
- Configuring BVSM User Roaming Preferences, page 3-13

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 3-2.

Figure 3-2 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, **10.120.3.62**.

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, **e3pgwcucmhwgrpclu1**.
- 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 BVSM and Cisco PGW.

To verify the values of the #CUSTDIALPLAN#, #EGRESSCUSTDIALPLAN#, and #COMMONLEGACYPBX# variables, 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-ENT3**.

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

BVSM does not assign media resource group lists directly to a location. BVSM 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 3-3.

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

Provider	Reseller	Customer
UKProvider	UKReseller1	UKCustomer1

Step 3 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **e3msClu1Cus1**
- Description—<*mediaservicedesc*>; for example, **City 4 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 3-4.

Figure 3-4 Adding Feature Groups—Customer Level (UKCustomer1)

Provider	Reseller	Customer
UKProvider	UKReseller1	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 BVSM User Roaming Preferences

If the BVSMUserRoaming 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 3-5.

Figure 3-5 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 3-6.

Figure 3-6 Adding Locations—Division Level (UKDivision1)

Provider	Reseller	Customer	Division
UKProvider	UKReseller1	UKCustomer1	UKDivision1

Step 3 From the Details menu, add the following:

- Location Name—<*LocationName*>; for example, **1631clu1cus1loc1**
- 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, **e3pgwcucmhwgrpclu1**
- PBX Template—Default.
- 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.

Step 4 Click **Next >>**.

Step 5 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, **4**
- Default Area Code—<*DefAreaCode*>; for example, **1631**

- 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 6 From the Subnets menu, enter the IP subnet assigned to Location <*LocSubnet*>; for example, **10.181.3.0**.

Step 7 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 8 Click **Next >>**.

Step 9 From the Line Number menu, enter the required number of lines for each line type; for example, **20**.

Step 10 From the Services menu, enter the required number of subscribers for each service; for example, **20**.

Step 11 Click **Next >>**.

Step 12 From the Media Services menu, enter the Name <*CorrectMediaService*>; for example, **e3msClu1Cus1**.

Step 13 From the Phone Types menu, enter the required number of phones for each phone type; for example, **20**.

Step 14 Click **Add**.

This procedure updates, BVSM, 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, **e3c1**.

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

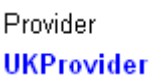
This section describes the steps required to move the inventory of E.164 numbers and phones created at the provider level to the customer locations.

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 is shown on the screen, as shown in Figure 3-7.

Figure 3-7 Moving Inventory of E.164 Numbers and Phones to Locations—Provider Level (UKProvider)



This section includes the following topics:

- Moving E.164 Number Inventory, page 3-19
- Moving Phone Inventory, page 3-20

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 > E164 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: 1631clu1cus1loc1**
- Start of number range—<*startofnumberrange*>; for example, **1631111000**
- End of number range—<*endofnumberrange*>; for example, **1631111019**

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: 1631clu1cus1loc1**

Step 5 Click **Next**.

Step 6 Choose a value for Subnet—<*locationsubnet*>; for example, **10.181.3.0**.

Step 7 Click **Move Phone**.

This procedure updates both BVSM 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 BVSM, 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 is shown on the screen, as shown in Figure 3-8.

Figure 3-8 Location Administration—Location Level (1631clu1cus1loc1)

Provider	Reseller	Customer	Division	Location
UKProvider	UKReseller1	UKCustomer1	UKDivision1	1631clu1cus1loc1

This section includes the following topics:

- Adding PSTN Published Numbers, page 3-21
- Adding Emergency Published Numbers, page 3-22
- Assigning Range of E.164 Numbers to Internal Numbers, page 3-23
- Registering Phones, page 3-25
- Adding an End User, page 3-26
- Adding User Extension Mobility, page 3-26
- Managing Phones, page 3-28
- Managing Users, page 3-29

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, **1631111009**

Step 5 Click **Add**.

This procedure updates both BVSM 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, **1631111008**.

Step 6 Click **Add**.

This procedure updates both BVSM and Cisco PGW.

Repeat this procedure for all required locations.

Assigning Range of E.164 Numbers to Internal Numbers

For a range of internal extensions, you can assign a range of E.164 numbers. These can then be assigned to IP phones so that users can make calls to the PSTN from those extensions. E.164 numbers can be associated with internal numbers by associating a range of 10^n numbers, where $n \in \{0,1,2,3,4\}$. The result is that a range of E.164 numbers is associated with a range of 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 preference LocationCentralPSTNAccessOnly is disabled
- Location is connected to the relevant Local Gateway Interface

- Range of E.164 numbers is assigned to a range of Internal numbers in ranges

For a range of internal extensions, the BVSM administrator can assign a range of E164 numbers. These can 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, the location preference AssociateFNNinRanges need to be changed first.

To change the AssociateFNNinRanges location preference, perform the following steps:

Procedure

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

Step 2 Choose a location for which you want to change the AssociateFNNinRanges preference and click **Preferences**.

Step 3 Click **AssociateFNNinRanges**.

Step 4 Choose **Available** to enable the setting.

Step 5 Click **Modify**.

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 **Range Assoc**.

Step 3 From the Select the Size of Range menu, enter the following:

- National Code—<*NatCode*>, select a national code; for example, **1631**
- Range Size—<*RangeSize*>; for example, **10**

Step 4 Click **Next >>**.

Step 5 From the Details menu, enter the following for the range:

- PSTN Number range—<*PSTNRange*>; for example, **1631111000-1631111009**
- Extension Number range—<*ExtRange*>; for example, **0200-0209**

Step 6 Click **Submit**.

Note To associate a range of numbers not equal to 10^n numbers, where n ε {0,1,2,3,4}, the second step needs to be repeated several times. For example, if a range of 21 numbers needs to be associated, this step needs to be repeated three times ($2x10^1 + 1x10^0$).

This procedure updates both BVSM and Cisco PGW.

Note The AssociateFNN-Ranges transaction is invoked only once.

Repeat this procedure multiple times if the range is not equal to 10^n numbers, where n ε {0,1,2,3,4} (as per the previous note), and for all required locations.

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**
- Choose Phone Feature Group—<*PhoneFeatureGroup*>; for example, **COS1International24Hour**

Step 4 Click **Next >>**.

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

- Softkey Template—<*SoftkeyTemplate*>; for example, **Softkey_Advanced**
- Device Use—<*Phone or Fax*>; for example, **Phone**

Step 6 From the Number Details menu, enter the following:

- Line Number—<*ExtOrE164*>; for example, **1631111001**
- Label—<*PhoneLabel*>; for example, **Desk4**

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

Step 7 Click **Register**.

This procedure updates both BVSM 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**
- 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 BVSM 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 From the Has Mobility menu, 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 1631111002**
- Label—<*PhoneLabel*>; for example, **user1**

Step 5 Click **Add**.

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

This procedure updates both BVSM 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 line(s)
- 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 BVSM 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, **clu1cus1loc1user1**.

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 BVSM and Unified CM.

CHAPTER 4

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 BVSM. 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, page 4-2
- Using Unmanaged PBX Devices, page 4-6
- Adding Unmanaged PBX Locations, page 4-8
- Adding PSTN Published Numbers, page 4-10
- Adding and Configuring Media Gateways, page 4-10
- Creating an E.164 Inventory, page 4-16
- Adding Emergency Published Numbers, page 4-16
- Assigning Range of E.164 Numbers to Internal Numbers, page 4-17
- Understanding Legacy PBX Information, page 4-19

Note The media gateways are not provisioned via BVSM; therefore, you must configure media gateways manually. For a sample configuration of a media gateway connected to a PBX using PRI QSIG, see Viewing a Sample Media Gateway Configuration, page 4-19.

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 is shown on the screen, as shown in Figure 4-1.

Figure 4-1 Adding IOS Device Components—Provider Level (UKProvider)

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 **IOS Device**.

Step 3 Click **IOS Device Types**.

Step 4 Click **Add**.

Step 5 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **C3845**
- Description—<*IOSDeviceTypeDesc*>; for example, **Cisco 3845**
- IOS Device Type (as referred to by Unified CM)—<*IOSCUCM*>; for example, **C3845**

- IOS Device Type (as referred to by Cisco PGW)—<*IOSPGW*>; for example, **C3845**.

Note For a list of supported external node types on the Cisco PGW, see Viewing Supported External Node Types on the Cisco PGW, page 4-23.

- Type—<*IOSorNonISR*>; for example, **ISR**

Step 6 From the Fixed Ports menu, enter the following:

- Number of Ethernet Ports—<*EthPorts*>; for example, **0**
- First Ethernet Port Number—<*FirstEthPort*>; for example, **0**
- Number of FastEthernet Ports—<*FastEthPorts*>; for example, **0**
- First FastEthernet Port Number—<*FirstFasEthPort*>; for example, **0**
- Number of GigabitEthernet Ports—<*GigEthPorts*>; for example, **2**
- First GigabitEthernet Port Number—<*FirstGigEthPort*>; for example, **0**
- Number of E1 WAN Ports—<*E1Ports*>; for example, **0**
- First E1 WAN Port Number—<*FirstE1Port*>; for example, **0**
- Number of T1 WAN Ports—<*T1Ports*>; for example, **0**
- First T1 WAN Port Number—<*FirstT1Port*>; for example, **0**
- Number of Analog Ports—<*AnPorts*>; for example, **0**
- First Analog Port Number—<*FirstAnPort*>; for example, **0**

Step 7 From the Network Module Slots menu, enter the following:

- Number of Network Modules Supported—<*NMs*>; for example, **4**
- First Network Module Slot Number—<*FirstNMSlot*>; for example, **1**

Step 8 Click **Add**.

Repeat this procedure for all IOS device types.

Adding IOS Device Network Modules

To add an IOS device network module, perform the following steps:

Procedure

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

Step 2 Click **IOS Device**.

Step 3 Click **IOS Device Network Modules**.

Step 4 Click **Add**.

Step 5 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **NM-HDV2-ISR**
- Description—<*IOSDeviceNMDesc*>; for example, **NM-HDV for ISR**

Step 6 From the Fixed Ports menu, enter the following:

- Number of Ethernet Ports—<*EthPorts*>; for example, **0**
- First Ethernet Port Number—<*FirstEthPort*>; for example, **0**
- Number of FastEthernet Ports—<*FastEthPorts*>; for example, **0**
- First FastEthernet Port Number—<*FirstFasEthPort*>; for example, **0**
- Number of GigabitEthernet Ports—<*GigEthPorts*>; for example, **0**
- First GigabitEthernet Port Number—<*FirstGigEthPort*>; for example, **0**
- Number of E1 WAN Ports—<*E1Ports*>; for example, **0**
- First E1 WAN Port Number—<*FirstE1Port*>; for example, **0**
- Number of T1 WAN Ports—<*T1Ports*>; for example, **0**
- First T1 WAN Port Number—<*FirstT1Port*>; for example, **0**
- Number of Analog Ports—<*AnPorts*>; for example, **0**
- First Analog Port Number—<*FirstAnPort*>; for example, **0**

Step 7 From the Interface Card Slots menu, enter the following:

- Number of Slots—<*ICs*>; for example, **1**
- First Slot Number—<*FirstICSlot*>; for example, **0**

- Interface Card Port Number Format—<*ICPortNumberFormat*>; for example, **module/slot/port**

Step 8 Click **Add**.

Repeat this procedure for all IOS device network modules.

Adding IOS Device Interface Cards

To add an IOS device interface card, perform the following steps:

Procedure

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

Step 2 Click **IOS Device**.

Step 3 Click **IOS Device Interface Cards**.

Step 4 Click **Add**.

Step 5 From the Details menu, enter the following:

- Name—<*uniquename*>; for example, **VWIC-2MFT-E1-DI**
- Description—<*IOSDeviceICDesc*>; for example, **VWIC-2MFT-E1-DI**

Step 6 From the Ports menu, enter the following:

- Number of Ethernet Ports—<*EthPorts*>; for example, **0**
- First Ethernet Port Number—<*FirstEthPort*>; for example, **0**
- Number of FastEthernet Ports—<*FastEthPorts*>; for example, **0**
- First FastEthernet Port Number—<*FirstFasEthPort*>; for example, **0**
- Number of GigabitEthernet Ports—<*GigEthPorts*>; for example, **0**
- First GigabitEthernet Port Number—<*FirstGigEthPort*>; for example, **0**
- Number of E1 WAN Ports—<*E1Ports*>; for example, **2**
- First E1 WAN Port Number—<*FirstE1Port*>; for example, **0**
- Number of T1 WAN Ports—<*T1Ports*>; for example, **0**

- First T1 WAN Port Number—<*FirstT1Port*>; for example, **0**
- Number of Analog Ports—<*AnPorts*>; for example, **0**
- First Analog Port Number—<*FirstAnPort*>; for example, **0**

Step 7 Click **Add**.

Repeat this procedure for all IOS device interface cards.

Using Unmanaged PBX Devices

This section describes how PBXs are defined in BVSM. 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.

The name of the provider is shown on the screen, as shown in Figure 4-2.

Figure 4-2 Unmanaged PBX Administration—Provider Level (UKProvider)

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**.

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, **e3pgwunmqsigwgrpcus1**
- Description—<*hwgrpdesc*>; for example, **City 3 "PGW-Unmanaged QSIG PBX" 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-ENT3**.

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 BVSM 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 3-7, Managing Customers, page 3-8, or Adding Divisions, page 3-14, before proceeding.

The PGW-Unmanaged PBX hardware group created in Adding Unmanaged PBX Locations, page 4-8 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 4-3.

Figure 4-3 Adding Unmanaged PBX Locations—Division Level (UKDivision1)

Provider	Reseller	Customer	Division
UKProvider	UKReseller1	UKCustomer1	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*>
- Hardware Group—<*unmpbxlocochwgrp*>; for example, **e3pgwunmqsigwgrpcus1**
- PBX Template—Default

Step 4 Click **Next >>**.

Step 5 From the Dial Plan menu, add the following:

- Site Code—<*LocSiteCode*>; for example, **411**
- Dial this to get an outside line—<*PSTNaccessprefix*>; for example, **9**
- Select extension number length—<*ExtLength*>; for example, **4**
- Default Area Code—<*DefAreaCode*>; for example, **1631**

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

- 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 internal extensions; for example, **20**.

Step 9 Click **Add**.

This procedure updates both BVSM and Cisco PGW.

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

Repeat this procedure for all required locations.

Adding PSTN Published Numbers

Note Ensure that you put the Cisco PGW in manual mode before proceeding with this step, and then take the Cisco PGW out of manual mode after this step is complete. If you do not, BVSM tries to invoke the AddPSTNPubNumber transaction on the Cisco PGW, which is not desirable. The PSTN published number should be added only to the BVSM database because the information is used in a later step.

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 3-21.

Adding and Configuring Media Gateways

This section describes the steps required to define and configure Cisco PGWs.

Defining Media Gateways

A media gateway is defined in BVSM as a Generic Cisco IOSDevice.

To define a media gateway, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Click **Add**.

Step 3 Click **Add** next to IOSDevice (Generic Cisco IOSDevice).

Step 4 From the Details menu, enter the following:

- Host Name—<*uniquename*>, *must* be same as the media gateway hostname; for example, **e4qsig2**
- Description—<*mediagatewaydescription*>; for example, **City 4 QSIG Voice Gateway 2**
- Country—<*CountrywhereGatewayis*>; for example, **United Kingdom**
- Device Type—<*DeviceType*>; for example, **C3825**

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

- IP Address—<*gatewayIP*>; for example, **10.190.4.40**
- Alternate IP Address—<*gatewayIP2*>; for example, **10.191.4.40**
- Config Password—<*configpassword*>; for example, **cisco**
- Enable Password—<*enablepassword*>; for example, **cisco**
- Version—<*gatewayIOSversion*>; for example, **IOSDevice: 12.x**
- Click **Manual Configuration Mode?**.
- E-mail address for Manual activation—<*email*>
- Click **Detailed trace file of configuration sessions?**.

Step 6 From the Roles menu, do the following:

- Click **PSTN Gateway**.
- Enter PSTN lines—<*PSTNlines*>; for example, **1000**.

Step 7 Click **Add**.

Repeat this procedure for all required media gateways.

Configuring Media Gateway Control Protocol

In Hosted UCS 5.1(b), signaling from the PBX is backhauled to the Cisco PGW via Media Gateway Control Protocol (MGCP).

To configure MGCP signaling, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Choose the gateway you want to configure.

Step 3 Click **Gateway Config**.

Step 4 Choose **MGCP** as the Gateway Protocol and click **Next >>**.

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

- UDP Port Number—<*UDPPort*>; for example, **7007**
- Protocol—<*Protocol*>; for example, **ETS_300_172**
- ISDN Side—<*NetworkUser*>; for example, **network**
- Domain Name—<*GatewayHostname*>; for example, **e4qsig**
- Voice Quality Monitoring Priority Value—<*VoiceQ*>; for example, **1**
- Transit Switch MGCP Configuration Template—<*MGCP_Template*>; for example, **MGCP_temp1**

Step 6 Click **Apply**.

Repeat this procedure for all required media gateways.

Configuring Network Modules used on the Media Gateway

To configure network modules used on the media gateway, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Choose the gateway you want to configure.

Step 3 Click **Network Module Mgt**.

Step 4 Choose the network module in us in the correct slot number; for example, choose **NM-HDV2-2T1/E1-E1-ISR** in **Slot Number 1**.

Step 5 Click **Update**.

Repeat this procedure for all required network modules and for all media gateways.

Configuring Interface Cards used on the Media Gateway

To configure interface cards used on the media gateway, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Choose the gateway you want to configure.

Step 3 Click **Network Module Mgt**.

Step 4 Click **Interface Cards**.

Step 5 For each device slot, select the interface card in use in the correct slot number; for example, for an NM-HDV2-2T1/E1-E1-ISR in Device Slot 1, choose **VWIC-2MFT-E1-DI** in **Slot Number 0**.

Step 6 Click **Update.**

Repeat this procedure for all required interface cards and for all media gateways.

Defining Media Gateway Ports and Trunks

To define a port used on the media gateway, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Choose the gateway you want to configure.

Step 3 Click **Port Management**.

Step 4 Click **Configure** next to the port you want to configure; for example, **Serial1/0/0 (E1)**.

Step 5 From the Port Configuration menu, enter the following:

- Codec Complexity—<*CodecComplex*>; for example, **flex**
- Framing—<*Framing*>; for example, **no-crc4**
- Line Code—<*LineCode*>; for example, **hdb3**
- Clock Source—<*ClockSource*>; for example, **line**
- DS0 Group—<*DS0Group*>; for example, **0**

Step 6 Click **Apply**.

To define a trunk used on the previously defined port, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Choose the gateway you want to configure.

Step 3 Click **Port Management**.

Step 4 Click **Configure** next to the port you want to configure; for example, **Serial1/0/0 (E1)**.

Step 5 Click **Trunk Config**.

Step 6 From the Trunk Configuration menu, enter the following:

- Switch Type—<*SwitchType*>; for example, **primary-qsig**
- Signaling Protocol—<*SigProtocol*>; for example, **QSIG**
- Use as—LegacyPBX

Step 7 Click **Next >>**.

Step 8 Click **Submit**.

Repeat this procedure for all required ports and trunks and for all media gateways.

Associating Media Gateways with the Cisco PGW

To associate media gateways with the Cisco PGW, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Click **Connectivity** next to the gateway you want to associate.

Step 3 Click **Gateway=>Transit**.

Step 4 Click **Connect** next to the Cisco PGW to which you want to associate the media gateway.

Repeat this procedure for all required media gateways.

Associating Media Gateways with Unmanaged PBXs

To associate media gateways with an unmanaged PBX, perform the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Click **Connectivity** next to the gateway you want to associate.

Step 3 Click **PBX Interconnect**.

Step 4 From the New Interconnects menu, enter the following:

- PBX Name—<*UnManPBX*>; for example, **cus1unmqsigpbx1**
- Gateway Port Id—<*RequiredPortId*>; for example, **Serial1/0/0**
- Transit Switch Config Template—<*ConfigTemplate*>; for example, **PBX_E1_Template1**

Step 5 Click **Connect**.

Repeat this procedure for all required media gateways.

This procedure updates both BVSM and Cisco PGW.

After a gateway or E1 has been provisioned into the Cisco PGW, BVSM does not put the associated functions into service. Similarly with deleting, BVSM does not take the required functions out of service, which allows the E1 or gateway to be removed from the Cisco PGW.

As a workaround, the service state must be manipulated manually on the Cisco PGW. For example, if the gateway name is e4qsig, the following commands are required after adding the first E1:

- **set-iplnk:iplnk1-e4qsig:IS**
- **set-iplnk:iplnk2-e4qsig:IS**

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.

For the procedures, see Creating an E.164 Inventory, page 3-3. To move the E.164 number inventory, see Moving E.164 Number Inventory, page 3-19.

Repeat this procedure for all required unmanaged PBX 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 calls is placed, the CgPN is replaced with the emergency published number. For the procedure, see Adding Emergency Published Numbers, page 3-22.

This procedure updates both BVSM 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 BVSM 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. E.164 numbers can be associated with internal numbers in two ways: by making a one-to-one mapping, or by associating a range of 10^n numbers, where n ε {0,1,2,3,4}. Both have the same end result (a range of E.164 numbers is associated with a range of internal numbers). The only difference is how the Cisco PGW is configured.

For the procedure, see Assigning Range of E.164 Numbers to Internal Numbers, page 3-22. This procedure updates both BVSM and Cisco PGW.

Note The AssociateFNN transaction is invoked multiple times. For example, if a range of ten numbers is associated, the AssociateFNN transaction is invoked ten times.

Repeat this procedure for all required unmanaged PBX locations.

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, the location preference AssociateFNNinRanges needs to be changed first.

To change the AssociateFNNinRanges location preference, perform the following steps:

Procedure

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

Step 2 Choose an unmanaged PBX location for which you want to change the AssociateFNNinRanges preference and click **Preferences**.

Step 3 Click **AssociateFNNinRanges**.

Step 4 Choose **Available** to enable the setting.

Step 5 Click **Modify**.

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 **Range Assoc**.

Step 3 From the Select the Size of Range menu, enter the following:

- National Code—<*NatCode*>, select a national code, for example, **1631**
- Range Size—<*RangeSize*>; for example, **10**

Step 4 Click **Next >>**.

Step 5 From the Details menu, enter the following for the range:

- PSTN Number range—<*PSTNRange*>; for example, **1631411000-1631411009**
- Extension Number range—<*ExtRange*>; for example, **000-009**

Step 6 Click **Submit**.

Note To associate a range of numbers not equal to 10^n numbers, where n ε {0,1,2,3,4}, the second step needs to be repeated several times. For example, if a range of 21 numbers needs to be associated, this step needs to be repeated three times ($2x10^1 + 1x10^0$).

This procedure updates both BVSM and Cisco PGW.

Note The AssociateFNN-Ranges transactions is invoked only once.

Repeat this procedure multiple times (if the range is not equal to 10^n numbers, where n ε {0,1,2,3,4}, as per the previous note) and for all required locations.

Understanding Legacy PBX Information

This section includes the following topics:

- Viewing a Sample Media Gateway Configuration, page 4-19
- Viewing Supported External Node Types on the Cisco PGW, page 4-23

Viewing a Sample Media Gateway Configuration

Following is a sample configuration for a media gateway connected to a PBX using PRI QSIG, backhauled to the Cisco PGW via MGCP. A Cisco 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.

```
e4qsig2#sh ver
Cisco IOS Software, 3800 Software (C3825-IPVOICEK9-M), Version
12.4(11)T3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 11-Jul-07 20:47 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

e4qsig2 uptime is 8 weeks, 6 days, 17 hours, 39 minutes
System returned to ROM by reload at 00:02:45 GMT Tue Dec 11 2007
System restarted at 21:40:07 GMT Mon Dec 10 2007
System image file is "flash:c3825-ipvoicek9-mz.124-11.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

e4qsig2#sh run
Building configuration...
```

```
Current configuration : 3068 bytes
!
! Last configuration change at 16:23:30 GMT Fri Dec 14 2007
! NVRAM config last updated at 14:49:06 GMT Fri Dec 14 2007
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname e4qsig2
!
boot-start-marker
boot system flash c3825-ipvoicek9-mz.124-11.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 server.mydomain.com
ip host pgw 10.121.4.12 10.120.4.12 10.121.3.12 10.120.3.12
multilink bundle-name authenticated
!
backhaul-session-manager
  set QSIG client ft
  group master set QSIG
  group slave set QSIG
  session group master 10.121.4.12 7007 10.190.4.41 7007 1
  session group slave 10.121.3.12 7007 10.190.4.41 7007 1
  session group master 10.120.4.12 7007 10.191.4.41 7007 2
  session group slave 10.120.3.12 7007 10.191.4.41 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 10.190.4.41 255.255.255.0
 duplex full
 speed 100
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.191.4.41 255.255.255.0
 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
```

Viewing Supported External Node Types on the Cisco PGW

To view the external node types supported on the Cisco PGW, log in to the Cisco PGW and execute the following:

```
cd /opt/CiscoMGC/etc
more extNodeTypes.dat
```

For example:

```
PGW-ENT5M% cd /opt/CiscoMGC/etc
PGW-ENT5M% more extNodeTypes.dat
::::::::::::::
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
LS1010  MGCP    SGCP
SCP     TCAPIP
TALISS7 SS7SG
MC3810  MGCP    IPFAS
SLT     BSMV0
H323    EISUP
UNKNOWN UNKNOWN
ITP     M3UA SUA
LIMD    LI
Unified CMCLUSTER  N/A
```

CHAPTER 5

Provisioning Cisco Unified MeetingPlace

This chapter describe how to integrate Cisco Unified MeetingPlace (MP) into the Cisco Hosted UCS architecture for providing audio conferencing and web collaboration. This chapter includes the following sections:

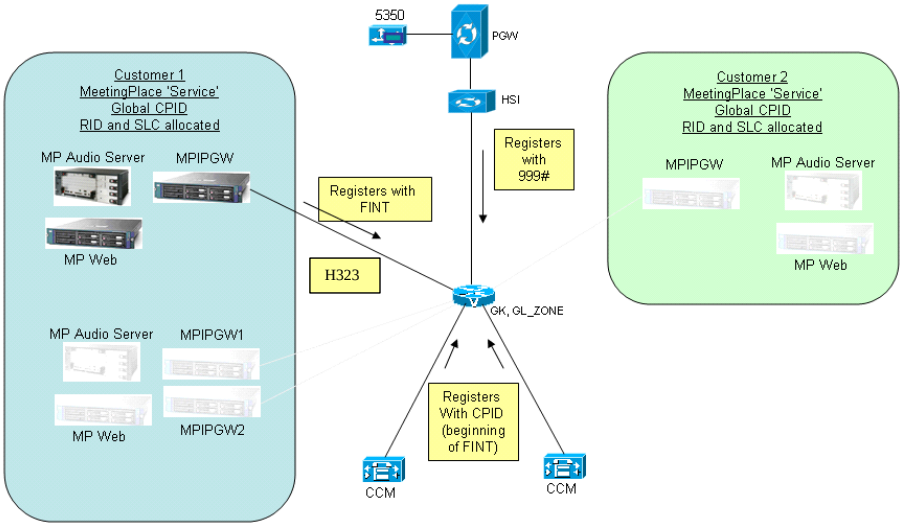
- Overview, page 5-1
- Using MeetingPlace Audio Server, page 5-5
- Using MeetingPlace IP Gateway, page 5-17
- Using MeetingPlace Web Conferencing, page 5-20
- Using MeetingPlace Directory Services, page 5-22
- Provisioning Cisco Unified Meeting Place, page 5-25

Overview

Unified CM servers register to the gatekeeper using the CPID of that Unified CM, and the HSIs register using 999# (which is defined as the default prefix). The zone used by both Unified CMs and HSIs is HUCS_ZONE.

MeetingPlace is integrated with Hosted UCS by using the same HUCS_ZONE zone and by registering the MeetingPlace IP Gateway using a FINT. With this design, the Cisco PGW routes to the MeetingPlace systems and the IP phone DNs both with FINTs. This creates a simple solution and allows the Cisco PGW dial plans to be used for MeetingPlace (see Figure 5-1.)

Figure 5-1 Gatekeeper Registration

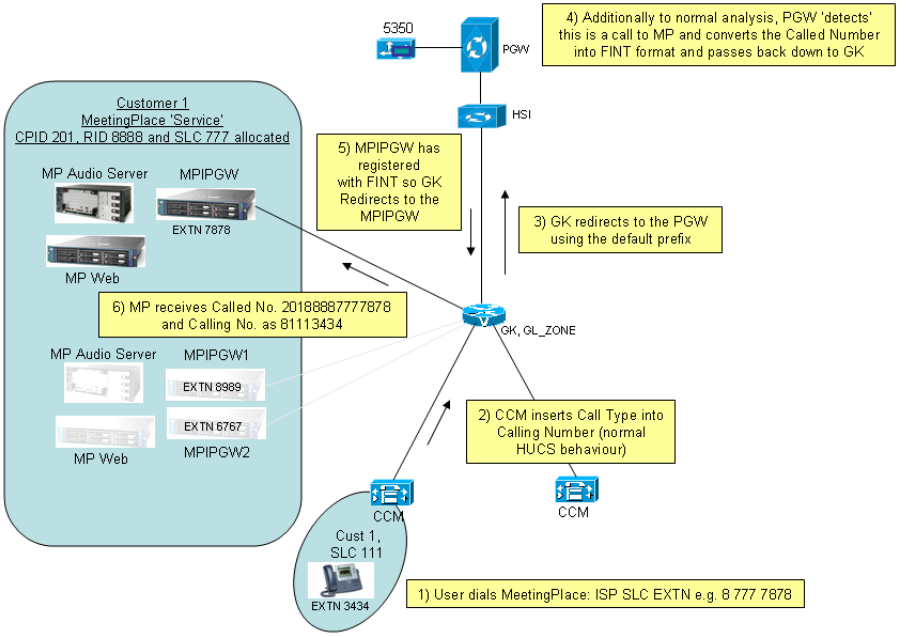


All MeetingPlace servers within a customer are defined with the same RID and SLC (RID assigned by BVSM and SLC assigned by the customer as normal). The servers are individually addressed using only the extension. The CPID has a single dynamically-assigned value for MeetingPlace, system-wide. This means that the FINT used by every MeetingPlace IPGW in the whole system contains the same CPID value. The CPID variable is called ICPID in the model rather than TCPID.

The RID is inherently unique system-wide because BVSM ensures that it is unique per CPID, and the CPID itself is globally allocated in this design to MeetingPlace. This allows the Cisco PGW to use CPID RID to identify calls from MeetingPlace and to identify the originating customer.

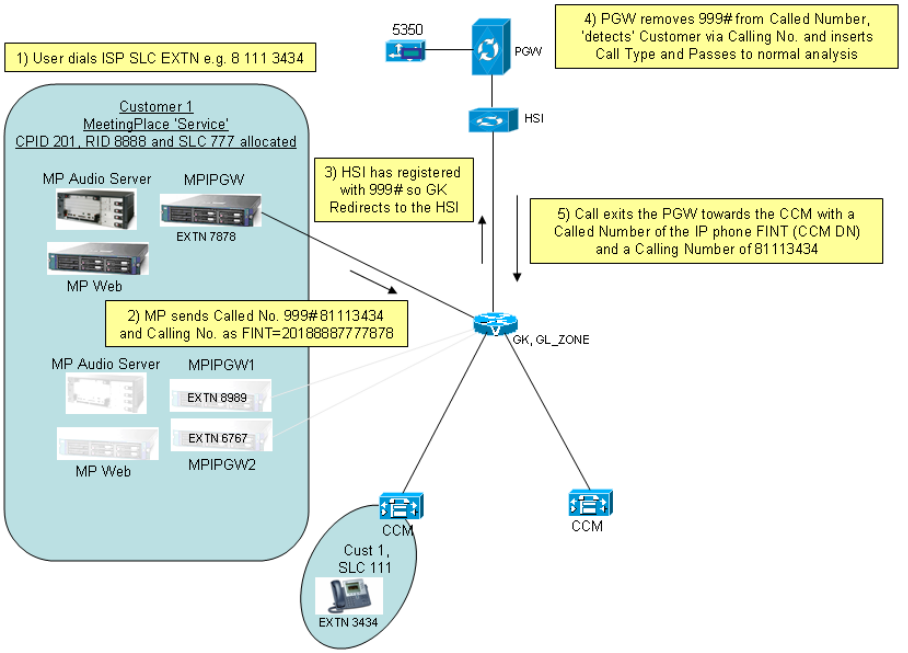
When an IP phone is used to dial into MeetingPlace, the user dials the inter-site prefix followed by the SLC for MeetingPlace, followed by the extension of the particular MeetingPlace server. Alternatively, an E.164 number can be used if it has been allocated for MeetingPlace. (See Figure 5-2.)

Figure 5-2 IP Phone to MeetingPlace Call using ISP



This integration also supports MeetingPlace out-dialing. The HUCS_ZONE on the gatekeeper already supports the 999# prefix as being the route to the Cisco PGW (through the HSI). To prevent misrouted calls, all MeetingPlace servers must be configured to prefix the called numbers with 999# to use the prefix defined for the zone and to correctly route calls towards the Cisco PGW. (See Figure 5-3.)

Figure 5-3 MeetingPlace Out-Dialing



BVSM uses the AssociateFNN transaction to associate internal extensions with E.164 numbers. This design allows the exact same transaction to be used to associate the MeetingPlace extensions with E.164 numbers. Consequently, MeetingPlace can dial out to the PSTN, call other on-net customers, and to place forced on-net calls. This design also supports dialing into MeetingPlace from the PSTN, from other on-net customers, and from users in the same customer dialing E.164 numbers to reach MeetingPlace (forced on-net).

Using MeetingPlace Audio Server

This section provides information about MeetingPlace Audio Server and includes the following topics:

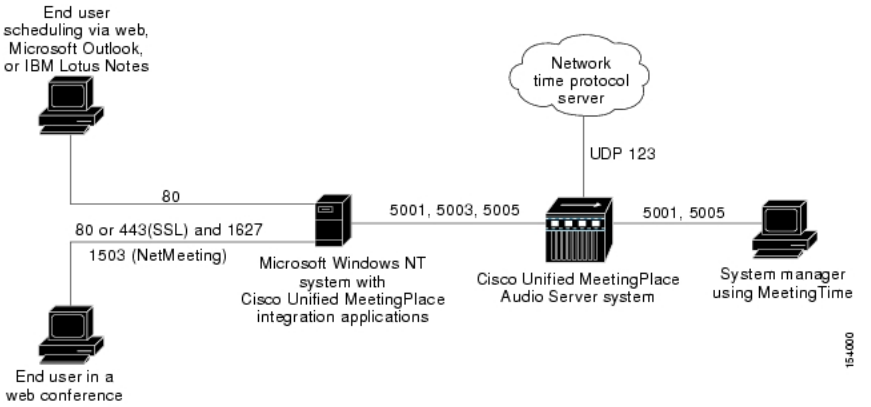
- Understanding LAN Port Details, page 5-5
- Understanding Serial Specifications for Audio Server, page 5-6
- Verifying the Software Release of the Audio Server, page 5-7
- Verifying the Status of the Audio Server Unit , page 5-8
- Configuring the Audio Server System LAN Parameters, page 5-9
- Configuring the Audio Server for Dialing Outbound, page 5-14

For more information, refer to the *Configuration Guide for MeetingPlace Audio Server Release 5.4* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/audio/54/cg/index.htm

Understanding LAN Port Details

To connect to other MeetingPlace components, such as MeetingPlace IP Gateway and MeetingPlace Web Conference Server, MeetingPlace Audio Server systems require certain TCP and UDP ports to remain open in the network. Figure 5-4 shows these details.

Figure 5-4 TCP and UDP Port Information



Understanding Serial Specifications for Audio Server

Run terminal emulation software on a PC and connect to the COM1 port of the CPU card using a null model cable. The terminal parameters to set are as shown in Figure 5-5.

Figure 5-5 COM Port Parameters

Parameter	Value
Baud Rate	19200
Data Length	8 bits
Parity	None
Stop Bits	1

The default username is *admin* and the default password is *cisco*.

Verifying the Software Release of the Audio Server

To access the CLI, use the Serial COM1 port or Telnet. After entering the username and password, the Audio Server displays the software release currently loaded:

```
Trying 10.11.214.50 ... Open
Release 5.4.1, May  4, 2007
user name: admin
Password:
Last login: Fri May  4 10:17:44 from default-gateway
*                              MeetingPlacehis
*
*                             by Cisco Systems
*
*
*
*               Copyright his 1993-2004 Cisco Systems, Inc.
*
*                           All rights reserved.
*
Conference server 5.4.1   S/N: JAB1050700A
Fri May  4 14:06:16 BST 2007
CiscoMtgPlace:tech$

Use the swstatus command for a more detailed display:
CiscoMtgPlace:tech$ swstatus
Conference server 5.4.1   S/N: JAB1050700A
System status: Operating
System mode: Up
Temperature: 32
Power supply: OK

MODULE NAME          STATUS     VERSION
SIM                  UP         "03/26/07 09:16 MPBUILD-R5_4_1_4"
LSH                  UP         "03/26/07 09:00 MPBUILD-R5_4_1_4"
SNMPD                UP         "03/26/07 09:27 MPBUILD-R5_4_1_4"
DBQSERVER            UP         "03/26/07 09:04 MPBUILD-R5_4_1_4"
DBSERVER             UP         "03/26/07 09:04 MPBUILD-R5_4_1_4"
POSERVER             UP         "03/26/07 09:12 MPBUILD-R5_4_1_4"
CPSERVER             UP         "03/26/07 09:10 MPBUILD-R5_4_1_4"
CONFSCHED            UP         "03/26/07 09:15 MPBUILD-R5_4_1_4"
WSSERVER             UP         "03/26/07 09:17 MPBUILD-R5_4_1_4"
VOICESERVER          UP         "03/26/07 09:24 MPBUILD-R5_4_1_4"
GWSIMMGR             UP         "03/26/07 09:31 MPBUILD-R5_4_1_4"

UNIT SITE  STATUS    RUN LEVEL  UNIT KIND   LAST ATTACH
```

```
  16     0  OK         UP          GATEWAY      05/11/07 15:16:44

CiscoMtgPlace:tech$
```

Verifying the Status of the Audio Server Unit

At the CLI, enter the **hwconfig**, **swstatus,** and **gwstatus** commands:

```
CiscoMtgPlace:tech$ hwconfig
Cabinet:                ELMA 4U
Bus architecture:       CompactPCI
Processor card:         SMM5370LATUDE S/N=7607855
    Processor:          Pentium III, Model 8, 700 MHz
    Memory:             512MB
    Temperature:        31C
    Voltages:           3.32V, 5.02V, 12.00V
Power Supplies:         OK
Fans :                   OK
SCSI Adapter :           NCR 810
    DISK 1:             36000MB (SEAGATE  ST373207LC       REV=0005)
    DISK 2:             36000MB (SEAGATE  ST373207LC       REV=0005)
Ethernet:               Intel 8225x PCI 10/100 (0001af181938)
Modem:                  Absent or unrecognized
MultiAccess Blades:
    Slot  6:            AC TP1610   (never came up)
Smart Blades:
    Slot  1:            NMS CG6000C S/N=105369683 REV=5894-B7 MSC0
PRC0
    Slot  2:            NMS CG6000C S/N=105369659 REV=5894-B7 MSC1
PRC1
CiscoMtgPlace:tech$

CiscoMtgPlace:tech$ gwstatus
Error: couldn't get status: error=0,count=0
Gateway SIM Status/Fri May  4 14:20:43 2007
Remote Units:
none found.
Gateways:
none found.
CiscoMtgPlace:tech$
```

The **gwstatus** command displays the status of the IP gateway. The snapshot above shows that the IP gateway is not reachable (because it has not been installed yet). To upgrade an Audio Server use the update along with update status commands as specified in the following installation and upgrade guide, see the following URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5782/c2001/Unified CMigration_09186a00806eb635.pdf

Configuring the Audio Server System LAN Parameters

Use the **getether** command to display the MAC address of the audio server, which is required for completing the configuration.

```
CiscoMtgPlace:tech$ getether
0001af181938
CiscoMtgPlace:tech$
```

Use the **net** command to display and modify the network settings:

```
CiscoMtgPlace:tech$ net
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select:
Select 1 to view the settings:
Select: 1
Current server configuration:
    Unit:                 #0 (CiscoMtgPlace)
    Active:               YES
    Description:          MeetingPlace
    Kind:                 Conference server
    IP Address:           10.11.214.50
    Ethernet address:     0001af181938
    NTP servers:          10.11.254.4
    Site:                 #0 (Cornwall)
    Site subnet mask:     255.255.255.0
    Site broadcast addr:  10.11.214.255
    Site default gateway: 10.11.214.1
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select:
```

Use the menus to modify the host and site names, the IP address and Ethernet (MAC) address, the subnet mask and broadcast address, site routing (default gateway) information, and the NTP configuration.

Note You must restart the Cisco Unified MeetingPlace system before some of the changes made by the **net** command can take effect. The system indicates whether you must restart the Cisco Unified MeetingPlace system.

Use the **timezone** command to set the time zone:

```
CiscoMtgPlace:tech$ timezone
Please select the region where this server is installed:
  1) Europe
  2) Far East
  3) North America
 99) quit
Select: 1
Please select the time zone for this server.

The following timezones are available:
  1) Europe/Amsterdam
  2) Europe/Brussels
  3) Europe/London
 99) no action
Select: 3

The local time zone (GMT) is 0 minutes west of GMT
Daylight savings time policy: Western Europe

Please confirm (y/n): y
DONE
CiscoMtgPlace:tech$

The date and time of the server must be set after the time zone is set
and only when the audio server is shut down by using the down command:
CiscoMtgPlace:tech$ down
Are you sure (y/n)? y
Checking to see if the system is loaded...OK
System DOWN procedure has been initiated.
The system is DOWN.
CiscoMtgPlace:tech$
CiscoMtgPlace:tech$ date
Tue May  8 12:22:03 BST 2007
CiscoMtgPlace:tech$
CiscoMtgPlace:tech$ date 0705081225
Tue May  8 12:25:00 BST 2007
```

```
CiscoMtgPlace:tech$
```

After setting the date, restart the audio server so that the date and time changes can take effect. Your connection to the server is lost while the server is restarting.

```
CiscoMtgPlace:tech$ restart enable
Are you sure (y/n)? y
Checking to see if the system is loaded...
The System Integrity Manager is not running.
Restarting the system...
[Connection to 10.11.214.50 closed by foreign host]
```

Set up the database structure depending on the blades available and the software licenses purchased:

```
CiscoMtgPlace:tech$ blade -his 120

This will reset many DB tables, are you sure?  (y/n) : y

Configuring 120 IP ports

Restart the system for changes to take effect
CiscoMtgPlace:tech$
```

Set up the multi-access blade after the database has been initialized using the **blade** command:

```
CiscoMtgPlace:tech$ blade

Slot    Card    Type    CardId  Ports
----    ----    ----    ------  -----
 1      CG6000C  SB       0
 2      CG6000C  SB       1
 3      no card
 4      no card
 5      no card
 6      TP1610   IP       0     0-119 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  1
Enter blade slot [1..6]:  6

  Blade Slot:   6
  MultiAccess Blade:    0
```

```
  Blade Installed:      TP1610
  Blade Configured:     TP1610-4

  IP Address [0]:               0.0.0.0
  IP Address [1]:               0.0.0.0
  Subnet Mask:                  0.0.0.0
  Default Gateway:              0.0.0.0
  Base Receive UDP Port [0]:    16390
  Base Receive UDP Port [1]:    16390
  Jitter Buffer Minimum Size:   100
  Jitter Buffer Optimization:   7
  IP Precedence:                0
  Type of Service (TOS):        0
  DSCP / DiffServ:              (unused)
  RTCP Interval:                (default)
  Port group:                   1
  Ports:                        0-119

Press <Enter> to continue...

Slot    Card    Type    CardId  Ports
----    ----    ----    ------  -----
 1      CG6000C  SB       0
 2      CG6000C  SB       1
 3      no card
 4      no card
 5      no card
 6      TP1610   IP       0     0-119 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..6]:  6

  Type                          [IP]:
  Card type                [TP1610-4]:  TP1610
  Port Group                     [ 1]:
  Number of Ports              [120]:
  1st Port                     [   0]:  23
  IP Address [0]            [0.0.0.0]:  10.11.214.51
  IP Address [1]            [0.0.0.0]:
  Subnet Mask               [0.0.0.0]:  255.255.255.0
  Default Gateway           [0.0.0.0]:  10.11.214.1
  Base UDP Port [0]           [16390]:
```

```
  Base UDP Port [1]          [16390]:
  Jitter Buffer Minimum Size  [100]:
  Jitter Buffer Optimization   [ 7]:
  IP Precedence                 [0]:
  Type of Service (TOS)        [ 0]:
  DSCP / DiffServ           [unused]:
  RTCP Interval            [default]:

Slot    Card    Type    CardId  Ports
----    ----    ----    ------  -----
 1      CG6000C  SB       0
 2      CG6000C  SB       1
 3      no card
 4      no card
 5      no card
 6      TP1610   IP       0     0-119 (10.11.214.51)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  1
Enter blade slot [1..6]:  6

  Blade Slot:   6
  MultiAccess Blade:    0
  Blade Installed:      TP1610
  Blade Configured:     TP1610

  IP Address [0]:               10.11.214.51
  IP Address [1]:               0.0.0.0
  Subnet Mask:                  255.255.255.0
  Default Gateway:              10.11.214.1
  Base Receive UDP Port [0]:    16390
  Base Receive UDP Port [1]:    16390
  Jitter Buffer Minimum Size:   100
  Jitter Buffer Optimization:   7
  IP Precedence:                0
  Type of Service (TOS):        0
  DSCP / DiffServ:              (unused)
  RTCP Interval:                (default)
  Port group:                   1
  Ports:                        23-142

Press <Enter> to continue...
```

```
Slot    Card    Type    CardId  Ports
----    ----    ----    ------  -----
 1      CG6000C  SB       0
 2      CG6000C  SB       1
 3      no card
 4      no card
 5      no card
 6      TP1610   IP       0     23-142 (10.11.214.51)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  x

Restart the system for any changes to take effect

CiscoMtgPlace:tech$ restart enable
Are you sure (y/n)? y
Checking to see if the system is loaded...OK
System DOWN procedure has been initiated.
CiscoMtgPlace:tech$
```

Configuring the Audio Server for Dialing Outbound

MeetingPlace can be set up for attendees to be dialed from the system to join conference calls, rather than the attendees having to dial in. To achieve this, digits must be prefixed to the front of the dialed number to enable the Hosted UCS system to route correctly within the H.323 zone.

The digits to be prefixed are 999#. The 999# prefix already resides on the gatekeeper to route towards the Cisco PGW (as a consequence of the HSI devices registering with 999#). The <CPID><RID> on the Calling Number is enough to determine the originating tenant.

The prefix must be manually configured in the audio server using the SuperUser account with the password of the day (POD). The POD can be retrieved from Cisco TAC.

Log in to the audio server and change to use the SuperUser account:

```
CORE-GSR-C>10.11.214.50
Trying 10.11.214.50 ... Open
```

```
Release 5.4.1, Jun  5, 2007
user name: admin
Password:
Last login: Tue Jun  5 11:03:28 from Unknown-HostName
*                             MeetingPlacehis
*
*                            by Cisco Systems
*
*
*
*               Copyright his 1993-2004 Cisco Systems, Inc.
*
*                          All rights reserved.
*
Conference server 5.4.1   S/N: JAB1050700A
Tue Jun  5 14:32:23 BST 2007
CiscoMtgPlace:tech$ su
Jun  5 2007
Password:
CiscoMtgPlace:csc$
```

Change the directory to /lat/etc and dump translation table 0 to a working file named for example, xtable0:

```
CiscoMtgPlace:csc$ cd /lat/etc
CiscoMtgPlace:csc$ pwd
/lat/etc
CiscoMtgPlace :csc$ xldump 0 > xtable0
CiscoMtgPlace:csc$ more xtable0
# Using database path: /lat/db/config
# Translation table 0
#
# From    To     Group          DestType        Comment
# ------------------------------------------------------
#
.*      \0      ANYGROUP        GENERIC         No translation

CiscoMtgPlace:csc$
```

Modify the working file using **vi** to update the To and Comment fields for the required translation. The modified file appears as shown below. The called number is perfixed with 999# for the gatekeeper to route the call to the PGW:

```
CiscoMtgPlace:csc$ more xtable0
# Using database path: /lat/db/config
# Translation table 0
#
# From    To        Group           DestType        Comment
```

```
# ----------------------------------------------------
#
.*      999#\0      ANYGROUP        GENERIC         Hosted
UCSTranslation

CiscoMtgPlace:csc$
```

To activate the new translation table, use an initialization command:

```
CiscoMtgPlace:csc$ xlinit xtable0 0

Processing translation table number 0
Saving current file /lat/etc/xtable.current-0
                in /lat/etc/xtable.current-old-0
Processing translation lines: 0 done
Notifying the cpserver modules....
Sending notification to unit 0:......Done
Done.

File xtable0 has been copied to /lat/etc/xtable.current-0

The digit translation utility completed.
NOTE: it may take a short while before the new table is used.

CiscoMtgPlace:csc$
```

Translation table 0 can be dumped to the screen to verify the activation:

```
CiscoMtgPlace:csc$ xldump 0
# Using database path: /lat/db/config
# Translation table 0
#
# From     To        Group           DestType       Comment
# ----------------------------------------------------
#
.*      999#\0       ANYGROUP        GENERIC        Hosted
UCSTranslation

CiscoMtgPlace:csc$
```

The translation can also be tested online:

```
CiscoMtgPlace:csc$ xltest 0
Using database path: /lat/db/config
Using Translation Table number 0

 Please Note: formatting characters are removed from string.

Line 1:         Hosted UCSTranslation
```

```
    Match:          .*
    Replace with:   999#\0
    Port group:     64188
    Dest Type:      GENERIC

Enter a number to be translated
901840123456

Number: 901840123456
Line=  1 (Index=  0)   Port Group=ANYGROUP DestType=GENERIC
Result=999#901840123456
Comment=        Hosted UCSTranslation

End of translation table.

CiscoMtgPlace:csc$
```

Using MeetingPlace IP Gateway

This section provides information about the MeetingPlace IP Gateway and includes the following topics;

- Installing the IP Gateway Software, page 5-17
- Setting up the IP Gateway, page 5-19

Installing the IP Gateway Software

For more information about installing IP gateway release 5.3.1.5, see the documentation for release 5.2.1 at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5780/c2001/Unified CMigration_09186a008032db07.pdf

Use an MCS server with Windows 2000 Server installed.

Download the IP gateway software from CCO and execute the setup to install the software. When the Gateway SIM screen appears, configure it as follows:

```
Server Name: Enter the hostname of the Audio Server: CiscoMtgPlace
Shadow Server: Leave blank
Client IP Address: IP Address of the MCS where Gateway SIM is
installed: 10.11.214.55
Transfer Destination: Leave blank
Link Encryption Disabled: Unchecked (enabled)
```

If the Gateway SIM settings must be amended after the initial install, the Gateway SIM must be deleted and re-added.

To achieve this, perform the following steps:

Procedure

Step 1 Stop the MeetingPlace Services by choosing **Start > Programs > Administrative Tools > Services**.

Step 2 To display the Gateway SIM settings, choose **Start > Programs > MeetingPlace Applications > MeetingPlace Gateway Configuration**.

Step 3 Choose the Gateway SIM in the left-hand window and click **Delete**.

Step 4 Click **Add** to re-add the Gateway SIM using the settings as described above.

The MeetingPlace Services must be restarted after the configuration has been completed.

When the Gateway SIM settings are correct, the audio server **gwstatus** command shows the association:

```
CiscoMtgPlace:tech$ gwstatus
Gateway SIM Status/Fri May 11 16:24:07 2007
Remote Units:
  Unit 16 Hosted UCS-mp-ipgw     v5.2.0.70      Ok          05/11/07
16:23:52

Gateways:
  Unit 16 IP Gateway       v5.3.1.5       Ok          05/11/07
16:22:49
CiscoMtgPlace:tech$
```

Setting up the IP Gateway

Further settings are required for setting up the H.323 configuration for connecting the IP gateway to the gatekeeper.

Access these settings by choosing **Start > Programs > MeetingPlace Applications > MeetingPlace Management.**

Double-clicking the MeetingPlace IP Gateway icon. However, if the system displays “Could not read MeetingPlace IP Gateway Management URL, edit the Registry settings as follows:

```
Start > Run:Regedit
Navigate to: \\HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\MeetingPlace IP
Gateway
Under General Settings:
Outdial Protocol: H.323
Under H.323 Settings:
H.323 Enabled: 1
E.164 Address: Number to be dialed for MP access:
<CPID><RID><SLC><EXTN> = <FINT>
H.323 ID: MP<SLC><EXTN>      {Is displayed on the IP phone when
out-dialing}
Gateway Port: 1720 (Decimal)
Gatekeeper Address: 10.11.214.37
Gatekeeper Port: 1719 (Decimal)
Use Gatekeeper: 1
```

The zone to register to on the gatekeeper is not configurable on the MPIPGW. In the Hosted UCS deployments, it should be the HUCS_ZONE to which the MPIPGW should register. Because it is not configurable on the MPIPGW, the gatekeeper(s) must be manually configured using the following Cisco IOS software command:

```
Gatekeeper
no zone subnet HUCS_OFFNET_ZONE <MPIPGW IP Address>/32 enable
```

This prevents the MPIPGW from registering with HUCS_OFFNET_ZONE and forces registration to HUCS_ZONE.

After these modifications and restarting the IP gateway server, a registration attempt is made to the gatekeeper. The gatekeeper should show the registration as shown in the following, with a Meeting Place system registered with a CPID of 201, RID of 8888, SLC of 777 and an EXTN of 1111:

```
GL-H6-GK#show gatekeeper endpoints
                    GATEKEEPER ENDPOINT REGISTRATION
```

```
                    ================================
CallSignalAddr   Port  RASSignalAddr    Port  Zone Name          Type
Flags
---------------- ----- --------------- ----- ---------          ----
-----
10.11.214.34     54428 10.11.214.34     54429 HUCS_ZONE
VOIP-GW
    H323-ID: GLH601-External_1
10.11.214.36     1720  10.11.214.36     33309 HUCS_ZONE
VOIP-GW E
    H323-ID: GL-H6-HIS
10.11.214.55     1720  10.11.214.55    1078  HUCS_ZONE           TERM

    E164-ID: 20188887771111
Total number of active registrations = 3

GL-H6-GK#
```

If a call is made from the solution through the gatekeeper and IP gateway to the MeetingPlace audio server, the MeetingPlace audio stream should be audible.

Using MeetingPlace Web Conferencing

This section describes the MeetingPlace Web Conferencing application and includes the following topics:

- Installing the Web Conferencing Server, page 5-20
- MeetingTime Information, page 5-21

Installing the Web Conferencing Server

For more information about installing the Web Conferencing Server, see the documentation at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5776/c2001/Unified CMigration_09186a00806e3b9e.pdf

After the web server is installed and the gateway SIM software is operational, the audio server shows the connectivity with the new web components:

```
CiscoMtgPlace:csc$ gwstatus
Gateway SIM Status/Tue Jun  5 16:33:58 2007
Remote Units:
```

```
  Unit 16 Hosted UCS-mp-ipgw     v5.2.0.70      Ok
06/05/07 16:33:52
  Unit 17 MPWEB            v5.2.0.70      Ok                    06/05/07
16:33:43

Gateways:
  Unit 16 IP Gateway       v5.3.1.5       Ok                    06/05/07
16:33:27
  Unit 17 WebPub:DataSvc   v5.4.156.0     Ok                    06/05/07
16:32:57
  Unit 17 WebPub:Audio     v5.4.156.0     Ok                    06/05/07
16:33:01
  Unit 17 DataConf:GW      v5.4.156.0     Ok                    06/05/07
16:33:53
  Unit 17 DataConf:GCC     v5.4.156.0     Ok                    06/05/07
16:33:09
  Unit 17 DataConf:MCS     v5.4.156.0     Ok                    06/05/07
16:33:05
  Unit 17 WebPub:Master    v5.4.156.0     Ok                    06/05/07
16:33:01
  Unit 17 WebPub:MPAgent   v5.4.156.0     Ok                    06/05/07
16:32:37
  Unit 17 MPConvert        v5.4.156.0     Ok                    06/05/07
16:32:37
CiscoMtgPlace:csc$
```

MeetingTime Information

MeetingTime is a desktop application through which you can access and configure the Cisco Unified MeetingPlace Audio Server system for all types of users, including end users, contacts, attendants, and system administrators. As a system administrator, you must have a copy of MeetingTime to manage and maintain the system. It is used to configure the system, run reports, monitor capacity, and run routine system management functions.

In addition, you may choose to deploy MeetingTime to other users, including help desk employees, department administrators, and qualified end users.

For information about installing MeetingTime software, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/audio/54/ag/54asag35.htm

Using MeetingPlace Directory Services

This section describes the MeetingPlace Directory Services and includes the following topics:

- Licensing MeetingPlace Directory Services, page 5-22
- Installing MeetingPlace Directory Services, page 5-23
- Using MeetingPlace Directory Services Administrator, page 5-24
- Understanding the Interaction with BVSM and LDAP, page 5-24
- Provisioning Cisco Unified Meeting Place, page 5-25

Licensing MeetingPlace Directory Services

Before installing the Directory software, the MeetingPlace Audio Server must be licensed to support the synchronization with Directory Services. The license information can be checked and updated via the MeetingTime application by completing the following steps:

Procedure

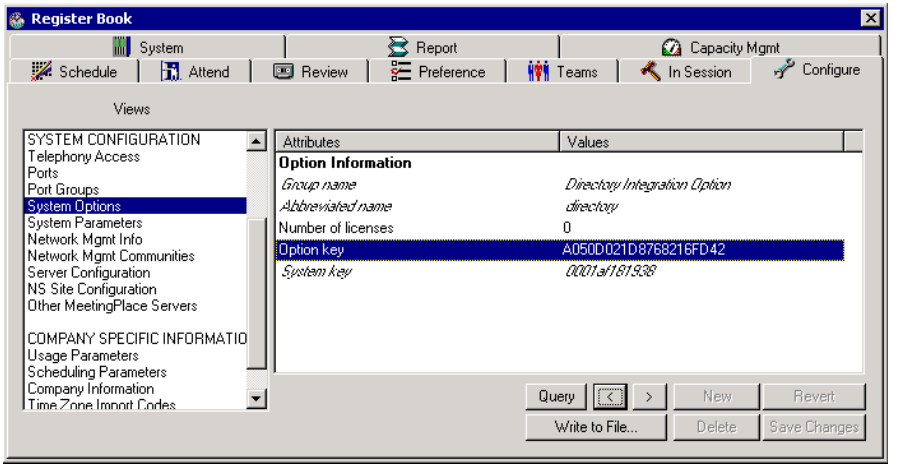
Step 1 In MeetingTime, choose **Options > Preferences** or click on the register book in the GUI to open the Register Book window.

Step 2 To verify the installed licenses, click the **Configure** tab, choose **System Options** in the left hand window, and click **Query** to retrieve the licenses from the MeetingPlace Audio Server.

The **< >** buttons can be used to scroll through the various licenses.

Figure 5-6 shows that this MeetingPlace system does not have a license for Directory Services.

Figure 5-6 Viewing Directory License Information via MeetingTime



After a license has been purchased, MeetingTime can be used to update the license information by inserting the new Option Key, changing the Number of Licenses to 1, and selecting the Save Changes button.

Installing MeetingPlace Directory Services

For information about installing MeetingPlace Directory services, see the *Administration Guide for Cisco Unified MeetingPlace Directory Services* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/mpds/54/ag/54dsag.pdf

MeetingPlace Directory software is typically installed on a dedicated server in a customer network, but it can also be installed on the same machine as the MeetingPlace IPGW or MeetingPlace Web server. In the POC, it was installed on the MeetingPlace Web server.

Before installing Directory Services, Java Runtime Environment (JRE) version 1.4.2_05 or later must be installed on the Directory Server.

After the MeetingPlace Directory Service software is installed, a MetaLink agreement must be established between the MeetingPlace Audio Server and the Directory Services Server. The *MeetingPlace Administration Guide* shows how to set this up and how to monitor the synchronization of data between them.

Using MeetingPlace Directory Services Administrator

After the software is installed and a MetaLink agreement is established between the MeetingPlace Audio Server and the Directory Services server, complete the following steps:

Procedure

Step 1 Choose **Start Menu > DC Directory Administrator**.

Step 2 In the log-on window, leave the Profile Name as Default Profile and click the **Next** button.

Step 3 In the next window, change the User Name to **/o=comp.com/cn=Admin** and use the password that was inserted at installation time, and click the **Finish** button.

A directory tree is displayed in the left-hand pane. This can be opened to display users that were entered into MeetingPlace (probably by using MeetingTime) and uploaded into the Directory Server via the MetaLink agreement synchronization.

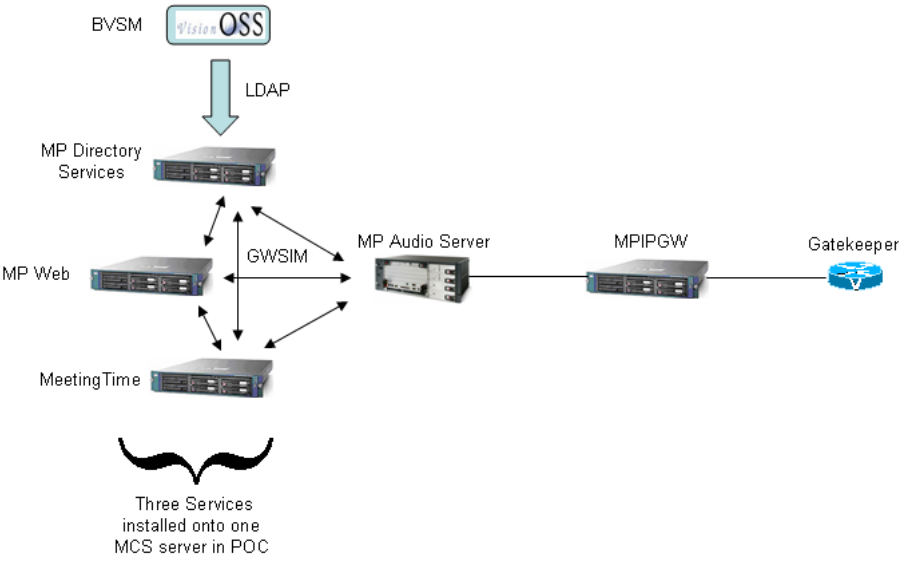
In the Hosted UCS solution, users are entered into the Directory Server by the VisionOSS BVSM platform (through LDAP), and the MetaLink synchronization process replicates this data into the rest of the MeetingPlace devices (through MP Gateway System Information Manager or GWSIM).

Understanding the Interaction with BVSM and LDAP

The devices within MeetingPlace (Audio Server, MeetingTime, Directory Services and MP Web) use MeetingPlace Gateway System Information Manager (MP GWSIM) to synchronize information. For example, after a user profile has been entered into one of the devices, GWSIM ensures that all devices are synchronized so that there is a single view of that user among all devices.

The user profiles are provisioned into the Directory Server by BVSM in Hosted UCS (via LDAP), and GWSIM ensures those user profiles are synchronized to the other MeetingPlace devices. (See Figure 5-7.)

Figure 5-7 LDAP Provisioning by BVSM



MeetingPlace uses the concept of user profiles and user groups. User groups are templates that user profiles can reference for ease of administration. If the use of user groups is required, these can be entered into the system manually using MeetingTime. These can then be referenced by BVSM in the user profiles using LDAP.

Provisioning Cisco Unified Meeting Place

This section includes the following topics:

- Provisioning a Cisco Unified MP Hardware Set, page 5-26
- Provisioning the Cisco Unified MP Directory Server, page 5-26
- Provisioning the Cisco Unified MP Directory Service , page 5-27

- Subscribing a Location to the Cisco Unified MP Directory Service, page 5-27
- Creating a Hardware Group for Unified CM, page 5-28
- Provisioning the Cisco Unified MP Conference Service, page 5-28

Provisioning a Cisco Unified MP Hardware Set

To provision a Cisco Unified MP hardware set, perform the following steps:

Procedure

Step 1 Choose a provider in BVSM.

Step 2 From the Dial Plan Tools menu, choose **Hardware Sets used by the provider** and click **PGW-Unified CM**.

Step 3 Click **CiscoMPDirectory** and click **Modify** to save changes.

Step 4 From the Hardware Set Management page, click the **Associated Dialplans** tab and disconnect and reconnect the dial plan.

Provisioning the Cisco Unified MP Directory Server

To provision the Cisco Unified MP directory server, perform the following steps:

Procedure

Step 1 From the Network menu, choose **Directory Server**.

Step 2 From the Manage Directory Server page, click **Add**.

Step 3 Next to the CiscoMPDirectory Server option, click **Add** and populate values.

Step 4 Verify the configuration by clicking **Test** for the Directory server created.

The Test button accesses the IP address. If this is successful, the username and password defined in the previous step are used to log in to the directory server and list all the domain/users under the directory.

Step 5 From the Network menu, go to **Gateways** and click the **Connectivity** tab next to the CiscoMPDirectory server created.

Step 6 Click the **Gateway => Transit** tab and connect.

Provisioning the Cisco Unified MP Directory Service

To provision the Cisco Unified MP directory service, perform the following steps:

Procedure

Step 1 From the Resources menu, choose **Directory Services**.

Step 2 Navigate to the correct reseller/customer.

Step 3 Click **Add** and populate values.

Step 4 From the General Administration menu, choose locations.

Step 5 Click **Add**.

Subscribing a Location to the Cisco Unified MP Directory Service

To subscribe a location to the Cisco Unified MP directory service, perform the following steps:

Procedure

Step 1 Choose the location that needs to be associated to the Directory Service.

Step 2 Click the **Advanced Mgt** tab.

Step 3 Click the **Directory Services Mgt** tab and connect.

Now when users are added, modified, or deleted under the location, the Directory Server is updated.

Creating a Hardware Group for Unified CM

To create the hardware group for Cisco Unified MP, perform the following steps:

Procedure

Step 1 From the Network menu, go to **Hardware Groups**.

Step 2 From the Hardware Group Management page, click **Add** to create a new hardware group.

Step 3 From the Available Transit Switches menu, choose **PGW**.

Step 4 From the Available PBX Devices menu, choose **Unified CM**.

Step 5 From the Available Conference Service menu, choose the **MeetingPlace directory server**.

Provisioning the Cisco Unified MP Conference Service

To provision the Cisco Unified MP conference service, perform the following steps:

Procedure

Step 1 From the Resources menu, choose **Conference Services** and add a service.

Step 2 Choose the previously-created hardware group.

Step 3 From the drop-down menu, choose the correct directory server.

Step 4 From the Resources menu, choose **E164 Inventory**.

Step 5 Choose country and national area code.

Step 6 Add the E.164 number range.

Step 7 Move the number range created to the MeetingPlace conference service.

Step 8 From the Resources menu, choose **Conference Service** and navigate to the conference service created in previous steps.

Step 9 Click the **PSTN Number Mgt** tab and associate the ranges allocated.

Step 10 Click the **PSTN Published Number** tab and assign a number.

Step 11 Click the **Pilot Number** tab and do the following:

a. Choose a pilot number from the drop-down menu.

b. Choose a time zone.

This step configures logic to the Cisco PGW to route incoming and outgoing calls from and to Unified CM.

CHAPTER 6

Provisioning Cisco Unity and Movius Voice Messaging Services

This chapter describes how to use BVSM to integrate Cisco Unity and Mereon IP Unity into the Cisco Hosted Unified Communications Services platform. This chapter includes the following sections:

- Provisioning Cisco Unity, page 6-1
- Provisioning Movius Servers, page 6-4
- Provisioning Movius AutoAttendant, page 6-15

Provisioning Cisco Unity

This section describes the steps required to provision Cisco Unity with BVSM for integration into the Cisco Hosted Unified Communications Services platform, Release 6.1(a).

To provision Cisco Unity, perform the following steps:

Procedure

Step 1 To add a voice-mail server on BVSM, choose **Network > VoiceMailServer > Add Unity Server** and use the standard configuration parameters.

The number of MWI ports and number of voice-mail ports is not relevant, but must high enough so that there are enough resources later for the voice-mail service (for example, 1000).

This updates BVSM only.

Step 2 Connect the voice-mail server to the Cisco Communications Manager cluster on BVSM.

This creates the MWI port on the Communications Manager cluster, and updates BVSM.

Step 3 Create a hardware group with the relevant Cisco PGW, Cisco Unity server and Cisco Unified Communications Manager (CM) on BVSM.

Step 4 Create a voice-mail service on BVSM by choosing **Resources > VoiceMail Services > Add VoiceMail Service**.

The number of ports is relevant because these are the ports used for calls to and from the voice-mail system.

On the Unified CM, this step creates the voice-mail ports (except for the MWI already created in step 2), line group, hunt list, and relevant CSSs and partitions.

This step also provisions the Cisco PGW, with the AddVMService-Unity transaction.

Inside this service you must provision the following:

a. Add VoiceMail Pilot.

This provisions the Unified CM with the hunt pilot and provisions the Cisco PGW (AddVMServicePilot-Unity transaction).

b. Associate DDI to VoiceMail Pilot number.

This provisions the Cisco PGW (AssociateFNN-Unity).

c. Add a published number.

This provisions the Cisco PGW (AddPSTNPubNum-Unity).

Step 5 Add a voice-mail service to a location in BVSM by choosing **General Administration > Locations > Advanced Mgt. > VoiceMail Mgt.**

This creates the voice-mail (VM) profile and the VM pilot on the Unified CM, and configures all the phones in that location with that profile.

Step 6 Choose **Manage Integration** and add an integration by doing the following:

a. Choose an SCCP integration.

b. Choose an integration name and use the name of the CallManager cluster used in BVSM.

c. Add the IP address of the server in the Unified CM cluster.

d. The MWI on and off devices are created with FINT *<CPID><reserved RID><reserved SLC><001=ON, 002=OFF>* as per the Movius design. The reserved RID=9999 and SLC=999.

   Using the same MWI devices as Movius ensures that Movius and Cisco Unity can co-exist while serving different customers or sites on a cluster.

e. The number of ports is the number of ports selected in step 4 plus one (the MWI port). The Unified CM device name prefix should be the name used in step 1 to create the VM Server followed by "-VI"; for example, **Unity-VI**.

f. Continue through the rest of default settings and complete the integration.

g. In the created integration, go to the Ports tab and enable all the ports.

   The first port must have only **Dialout MWI** checked, and the rest must have **Answer Calls** and **Message Notification** checked.

Step 7 Add voice mail to a user on BVSM by doing the following:

a. After a user is created and a phone or extension mobility is associated to this user, click the **VoiceMail** button and create a voice-mail account. This provisions Unity with user information.

b. After creating a user, go to the Cisco Unity Administrator and verify the following:

   – The subscriber created is usable.

     If the name of the user has previously been used in the exchange server to which the Unity Server is connected, the user will not be usable. If so, the easiest option is to delete the voice-mail account of that user on BVSM, delete the used name on the Active Directory, and then add the voice-mail account again. The other option is to import the user from AD to Unity.

   – Verify that the Switch tab in the subscriber is using the integration created in step 6.

Provisioning Movius Servers

This section describes how to use BVSM to provision Movius servers (IP Unity) for integration into a Hosted UCS 6.1(a) platform. In the example used in this section, a voice-mail service is being created for the Acme bank for provider GlobalProvider (GP).

This chapter contains the following sections:

- Using Static Configuration, page 6-4
- Using Network Configuration, page 6-7
- Configuring Additional Resources, page 6-10
- Adding Voice-Mail Service to a Location, page 6-14

Using Static Configuration

This section includes the following topics:

- Configuring a Virtual IP Address on the Cisco PGW, page 6-4
- Static Cisco PGW Configuration for Movius Servers, page 6-5
- Configuring the Movius Unified Messaging Server, page 6-5
- Configuring Changes to the the Movius Server Model Loader, page 6-6

Configuring a Virtual IP Address on the Cisco PGW

To use a redundant Movius system, the Cisco PGW is configured with a virtual IP address (for example, 10.100.98.90, which is the IP address of Movius) to which the PSTN gateway (Cisco PGW) sends SIP INVITE messages. In addition, the MGCdomain for the trunk group is set to a name (for example, *pgw*) that Movius uses when communicating with the Cisco PGW.

The following is an example of setting the virtual IP Address on Cisco PGW:

```
GL-H6-PGW>su
Password: cisco
# cd ../etc
#pwd
/etc
# vi hosts
```

```
#
# Internet host table
#
127.0.0.1       localhost
10.11.214.35    GL-H6-PGW       loghost
10.100.98.90   dept1-UM-1-------‡ add new entry
#
```

Static Cisco PGW Configuration for Movius Servers

You must manually configure a SIP path on the Cisco PGW to Movius. A Cisco PGW route list called *rtlist2ipunity* must exist in the configuration if the BVSM applied logic is later to be successfully applied.

Note the following example:

```
prov-sta::srcver="active",dstver="static-config-ipunity",confirm
prov-add:sippath:name="sip2unitypath1",mdo="IETF_SIP",desc="signaling
service from Unity to PGW"
prov-add:siplnk:name="sip-lnk-1",port=5060,pri=1,svc="sip2unitypath1",
ipaddr="IP_Addr1",desc="siplnk1 Unity to Pgw"
prov-add:trnkgrp:name="3001",svc="sip2unitypath1",type="SIP_IN"
prov-add:trnkgrpprop:name="3001",custgrpid="IUnified
CM",MGCDomain="pgw",MGCSipVersion="SIP/2.0",LocalPort="5060",Support18
3="3"
prov-add:trnkgrp:name="3002",svc="sip2unitypath1",type="IP_SIP"
prov-add:trnkgrpprop:name="3002",MGCSipVersion="SIP/2.0",LocalPort="50
60",Support183="3"
prov-add:siprttrnkgrp:name="3002",srvrr=0,cutthrough=2,version="2.0",e
xtsupport=1,sipproxyport=5060,url="10.100.98.90"
prov-add:rttrnk:name="rte2ipunity",trnkgrpnum=3002,weightedtg="OFF"
prov-add:rtlist:name="rtlist2ipunity",distrib="OFF",rtname="rte2ipunit
y"
prov-ed:trnkgrpprop:name="3002", UnsolicitedNotifyMethod="1"
```

For DTMF digits (such as the voice-mail password) to reach the Movius server, the SIP trunk *to* the Movius server must have the "UnsolicitedNotifyMethod" set to "1". For example:

```
prov-ed:trnkgrpprop:name="3002", UnsolicitedNotifyMethod="1"
```

Configuring the Movius Unified Messaging Server

The corresponding the Movius server configuration consists of the following two parts:

- The /etc/host files on each Unified Messaging (UM) server must be set up to resolve *pgw* to the four IP addresses of the Cisco PGW interfaces; for example:

```
# ifconfig -a
lo0:flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
index 1
        inet 127.0.0.1 netmask ff000000
eri0:flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500
index 2
        inet 10.11.214.35 netmask ffffff00 broadcast 10.11.214.255
        ether 0:3:ba:2f:ea:2c
#
```

- On the Movius UM server, the Cisco PGW interface must be resolved to *pgw*.

```
10.11.214.35 pgw
```

Configuring Changes to the the Movius Server Model Loader

To configure changes to the Movius model loader, perform the following steps:

Procedure

Step 1 Load the Movius Model IPUnity_Any by choosing **Dialplan Tools > Configuration Models > Load IPUnity models**.

Note The Movius messaging server is also known as IP Unity.

Step 2 Browse for the bulk loader being used and click **Upload file**.

This loads the IPUnity_Any worksheet from the above workbook.

A model change was also required to cater for a new Centrex ID that would be provisioned; as such, verify whether the following is present in the Movius server model:

AddVMServicePilot	IPUnity_model_xml	<centrixId>#CENTREXID#</centrixId>
AddVMServicePilot	IPUnity_model_xml	<tuiId>1</tuiId>

Using Network Configuration

This section includes the following topics:

- Adding the Movius VoiceMail Server, page 6-7
- Associating the Cisco PGW with other Cisco PGWs, page 6-8
- Associating Unified CM Clusters with other Unified CM Clusters, page 6-9
- Connecting the Movius Server to the Cisco PGW, page 6-9
- Connecting the Unified CM Clusters to the Cisco PGWs, page 6-9

Adding the Movius VoiceMail Server

To add the Movius VoiceMail server, perform the following steps:

Procedure

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

Step 2 Click **Add**.

Step 3 Click **Add IP Unity**.

Step 4 Enter the following:

- Host Name—**Test-Movius**
- IP Address—**10.120.5.97**]
- Description—**Test IP Unity Server**
- Config User Name—**system**
- Config Password—**movius**
- Software Version—**IPUnity: Any**

- Maximum Lines supported—**80000**

Adding the Movius Hardware Group

To add a Movius server hardware group, perform the following steps:

Procedure

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

Step 2 Add a hardware group that has the Movius Server, the Cisco PGW to which it will connect, and one Unified CM cluster.

There is a limit on the hardware group on BVSM. There can be only one Cisco Communications Manager (CM) cluster as part of a hardware group. Because voice mail is required for all clusters, create another hardware group including all other Unified CM clusters.

Associating the Cisco PGW with other Cisco PGWs

This step is required only if there is more than one Hosted UCS Cisco PGW pair. To associate the Cisco PGW with other Cisco PGWs, perform the following steps:

Procedure

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

Step 2 Click the **Associated Devices** button of the Cisco PGW used in 18.2.1.

Step 3 Click **Add** and enter the following:

- Set Name—**PGW-AssociatedSetVM**
- Description—**PGW-AssociatedSetVM**
- Transaction Type—**Add VoiceMail Service**
- Choose the remaining Cisco PGWs

Associating Unified CM Clusters with other Unified CM Clusters

This step is required only if there is more then one Unified CM cluster. To associate Unified CM clusters with other Unified CM clusters, perform the following steps:

Procedure

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

Step 2 Click the **Associated Devices** button of the Unified CM cluster used in 18.2.1.

Step 3 Click **Add** and enter the following:

- Set Name—**Unified CM-AssociatedSetVM**
- Description—**Unified CM-AssociatedSetVM**
- Transaction Type—**Add Voice Mail Service Pilot**
- Verify the remaining Unified CM Clusters.

Connecting the Movius Server to the Cisco PGW

To connect the Movius server to the Cisco PGW, perform the following steps:

Procedure

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

Step 2 Click the **VM Server => Transit** button of the Movius Server.

Step 3 Connect the Movius server to the Cisco PGW used in the Movius hardware group (if there is more than one Cisco PGW).

Connecting the Unified CM Clusters to the Cisco PGWs

Connecting the Unified CM clusters to the Cisco PGWs is needed only for Movius voice mail:

- ConnectIPPBXTransit—Add per-Unified CM cluster support for MWI signals when Cluster is connected to Cisco PGW that is directly connected to Movius.
- RemConnectIPPBXTransit—Add per-Unified CM cluster support for MWI signals when Cluster is connected to Cisco PGW that is indirectly connected to Movius (Cisco PGW with Movius connection).

To connect the Unified CM clusters to the Cisco PGWs, perform the following steps:

Procedure

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

Step 2 Click the **Connectivity** button of the Unified CM cluster used in 18.2.1.

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

Step 4 Click the **Connect** button of the Cisco PGW used in 18.2.1.

Repeat this step for every Unified CM cluster directly connected to the Cisco PGW used in 18.2.1.

The Unified CM clusters connected to the Cisco PGWs that are indirectly connected to the Movius server (via the Cisco PGW used in 18.2.1), should be connected to the Cisco PGWs to which they are directly connected.

Configuring Additional Resources

This section includes the following topics:

- Creating Voice-Mail Service for Customer, page 6-11
- Allocating the Internal Number for the Voice-Mail Pilot, page 6-11
- Adding the Voice-Mail Service Pilot Number, page 6-12
- Moving the E.164 Number Range for Voice Mail, page 6-12
- Associating the E.164 Number with the Voice Mail Pilot, page 6-13
- Adding the Published Number, page 6-13

- Adding Support for Multiple Classes of Service, page 6-14

Creating Voice-Mail Service for Customer

To create voice mail service for the customer, perform the following steps:

Procedure

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

Step 2 Click **Add** and enter the following:

- Name—**VM_Acme**
- Description—**VM_Acme**
- Country—**United Kingdom**
- Site Code—**999**
- VoiceMail Server Hardware Group—**E5HWGRPVM**
- Extension Length—**4**

Step 3 Click **Next.**

Step 4 To associate an E.164 to the voice-mail pilot later on so that PSTN can dial into voice mail, enter the national code **1630**.

Allocating the Internal Number for the Voice-Mail Pilot

To allocate the internal number for the voice-mail pilot, perform the following steps:

Procedure

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

Step 2 Click **VM_Acme**.

Step 3 Click the **Internal Number Mgt** button.

Step 4 Click **Allow** next to the Internal Number 000.

Adding the Voice-Mail Service Pilot Number

To add the voice-mail service pilot number, perform the following steps:

Procedure

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

Step 2 Click **VM_Acme**.

Step 3 Click the **Pilot Number** button and enter the following:

- Choose Pilot Number—**Extension Number 000**
- Domain Name—**abbey.com**; unique to a customer

This is the step where Cisco PGW, Unified CM, and Movius are actually provisioned with the per-customer Organization in Movius and the associated logic to route calls to it. The AddVMServicePilot mml script is used.

Moving the E.164 Number Range for Voice Mail

To move the E.164 number range for voice mail, perform the following steps:

Procedure

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

Step 2 Choose **UK**.

Step 3 Click **Next**.

Step 4 Choose National Area Code—**1630**.

Step 5 Click **Next**.

Step 6 Click the **Move Number Range** button and enter the following:

- Choose Location—**GP Sales: Acme National: VM_Acme: VM_Acme**

- Start of Number Range—**1630111990**
- End of Number Range—**1630111999**

Step 7 Click **Move**.

Associating the E.164 Number with the Voice Mail Pilot

To associate the E.164 number with the voice-mail pilot, perform the following steps:

Procedure

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

Step 2 Click **VM_Acme**.

Step 3 Click the **PSTN Number Mgt** button.

Step 4 Click **Allow** next to the Internal Number 000.

Step 5 An optional step is to associate an E.164 number with the voice-mail pilot. This allows external access to voicemail from the PSTN.

This procedure updates the Cisco PGW using the AssociateFNN-VM mml template

Adding the Published Number

To add the published number, perform the following steps:

Procedure

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

Step 2 Click **VM_Acme**.

Step 3 Click the **PSTN Published number** button.

Step 4 Enter a PSTN published number—**1630111000**.

Step 5 Click **Add**.

Adding Support for Multiple Classes of Service

To add support for multiple classes of service, perform the following steps:

Procedure

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

Step 2 Click **VM_Acme**.

Step 3 Click the **VoiceMail Profile Mgt** button.

Step 4 Click the **BasicVoiceMail**.

Adding Voice-Mail Service to a Location

To add voice-mail service to a location, perform the following steps:

Procedure

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

Step 2 Click **Acme_City5_C1**.

Step 3 Click the **VoiceMail Mgt** button.

Step 4 Click **Add** and enter the following:

- Name—**VM_City5C1**
- VoiceMail Service—**VM_Acme**
- Click **Next**.
- VoiceMail Pilot Number—**Extension Number 000**

Step 5 Click **Add and Enable.**

This procedure updates the Voice Mail profile in Unified CM for the location that will allow IP phones message button to automatically dial Movius, and Cisco PGW using the AddLocationVM mml script.

Because of AXL API limitations, BVSM cannot create the MWI On and MWI Off devices in Unified CM.

To determine these numbers, log into Cisco PGW as *mgcusr*, change directory to ../etc/cust_specific, and execute the following command to determine the MWI On and MWI Off numbers per cluster:

```
gl-mt-sp-pgw1% grep "MWI O" *
15409aaaaaa:; 001 Constant Digit string used within the "MWI On"
number. The MWI On number on each cluster will be 011999999001
15409aaaaaa:; 002 Constant Digit string used within the "MWI Off"
number. The MWI Off number on each cluster will be 011999999002
```

For each Unified CM cluster, you must manually create an MWI ON and MWI Device with these numbers. These numbers should be configured in the AllowMWI partition and the Output CSS should be set to IncomingToCluster because this allows the devices to turn any IP Phone MWI light on or off.

Provisioning Movius AutoAttendant

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 AutoAttendant functionality. Licenses are required for AutoAttendant functionality.

BVSM performs the provisioning of the telephony part for AutoAttendant, for example, creating an AutoAttendant service and associating a pilot number for it. All Auto Attendant related configurations including setting AutoAttendant 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 AutoAttendant:

- AutoAttendant in Hosted UCS is based on Location and is dependent on Voicemail. For a location to have AutoAttendant, it must have Voicemail.
- AutoAttendant uses the same Voicemail SLC (Site Location Code)
- Multiple Pilot numbers can be assigned per AutoAttendant.
- AutoAttendant 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 AutoAttendant
- Go Back to previous Menu
- Do Nothing
- Invalid Option

Auto Attendant Provisioning is carried out in the following phases:

- Configuring BVSM for Movius AutoAttendant, page 6-16
- AutoAttendant configuration on Movius web GUI

Configuring BVSM for Movius AutoAttendant

Note To create an AutoAttendant Service in a location, that location needs to have a VoiceMail Service. So you must complete all the steps in "Adding the Movius VoiceMail Server" section on page 6-7, "Allocating the Internal Number for the Voice-Mail Pilot" section on page 6-11, "Adding the Voice-Mail Service Pilot Number" section on page 6-12, and "Moving the E.164 Number Range for Voice Mail" section on page 6-12 before you begin creating an AutoAttendant Service Pilot for a location.

This section includes the following topics:

Adding AutoAttendant Service, page 6-17

Adding AutoAttendant Service

For each customer that requires VoiceMail support, a VoiceMail service is created. To define a VoiceMail Service, use the following procedure:

Procedure

Step 1 Choose **Resources > AutoAttendant Services**

Step 2 Click **Add**.

Note Make sure that you are adding a VoiceMail Service for the correct customer. The name of the customer will be displayed on the screen.

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

- Name: <uniquename>, for example, e3AutoAttendantServiceCus1
- Description: <VMServicedescription>, 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

Step 4 Click **Next >>**.

Step 5 Under **Details**, enter the following:

Step 6 IVR Server: <VMServer>, for example: MoviusforCity3

Step 7 Click **Next >>**.

Adding a Voicemail / AutoAttendant Server

To add a VoiceMail or AutoAttendant server, use the following procedure:

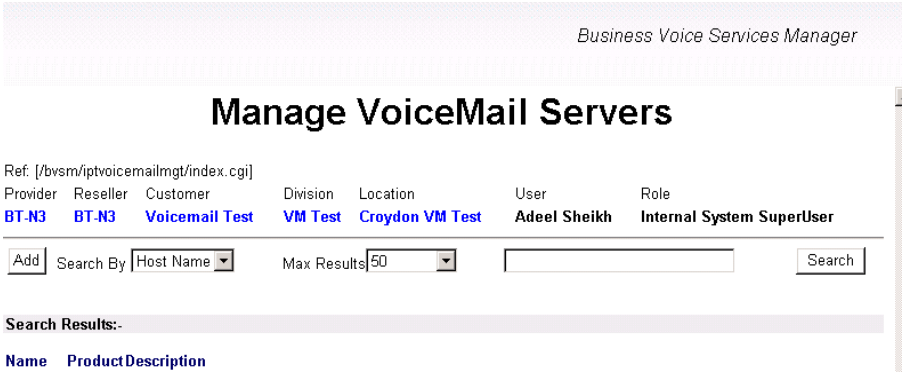
Procedure

Step 1 Navigate to the Network on the left hand menu.

Step 2 Click on the VoiceMail server.

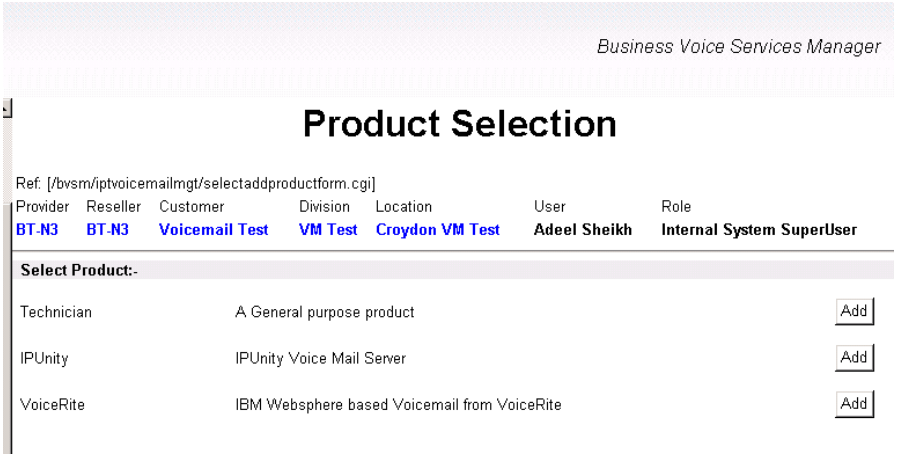
Step 3 Click **Add** to add a server in the network elements..

Figure 6-1 Adding a VoiceMail Server



Step 4 Select the product type called “IP Unity” and click **Add**.

Figure 6-2 Selecting the Product



Step 5 Enter Hostname, IP address, User name, config password and other details for the Voicemail server or AutoAttendant.

Step 6 If the Voicemail server and AutoAttendant Server are the same, check the IVR checkbox on the same screen.

Adding Voicemail Service for a Customer

To add a VoiceMail Service for a customer, use the following procedure:

Procedure

Step 1 Navigate to the customer for whom you want to create a Voice mail service.

Step 2 Go to the 'Resources' option on the BVSM menu on your left.

Step 3 Click on VoiceMail service.

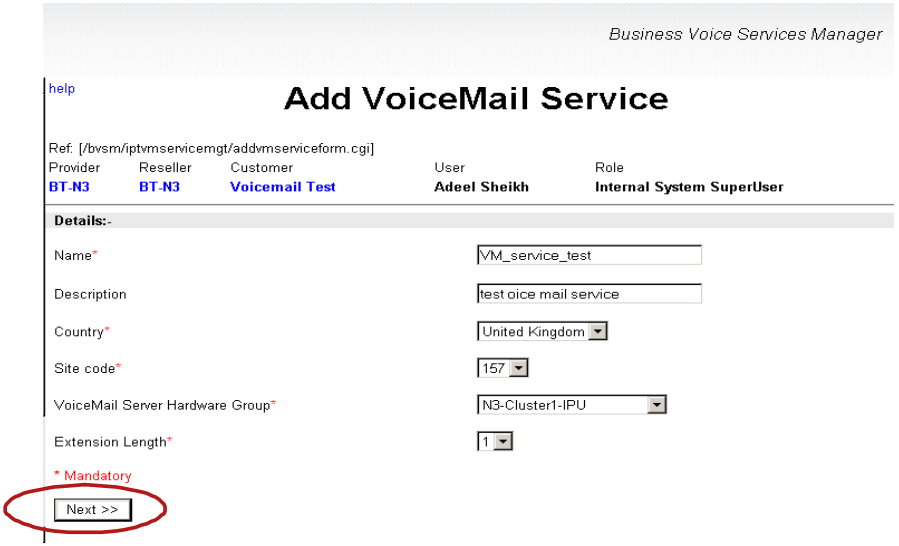
Step 4 Click **Add** to create a VoiceMail Service.

Step 5 Provide the following details:

- Name: Enter the name.
- Description: Enter the desrcription.
- Country: Select the country from the drop-down list box.

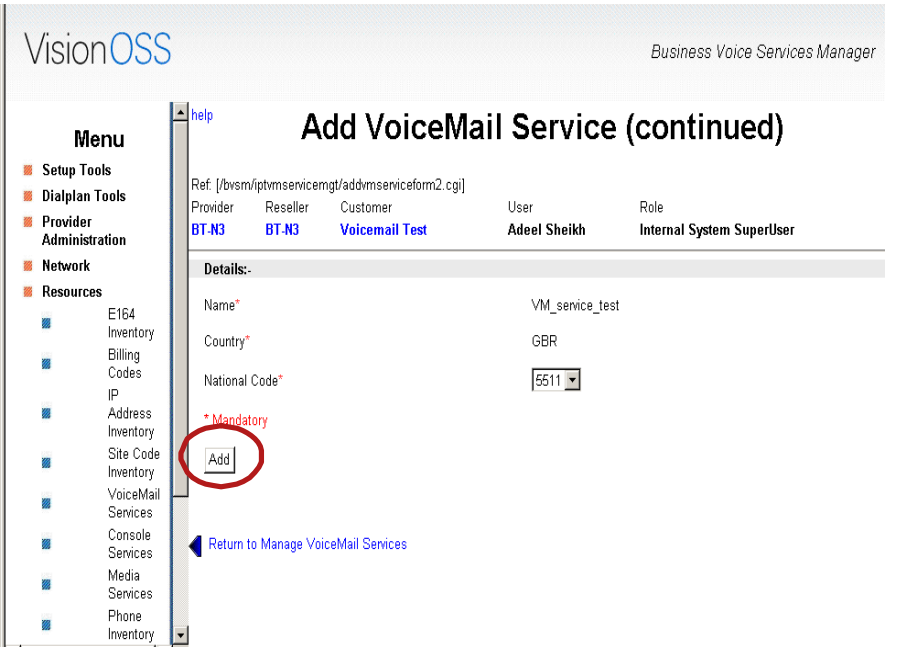
- Site code: Select the Site code from the drop-down list box.
- VoiceMail Server Hardware Group: Select the VoiceMail Server Hardware Group from the drop-down list box.
- Extension Length: Select the Extension Length from the drop-down list box.

Figure 6-3 Adding a VoiceMail Service



Step 6 Click **Next >>**.

Figure 6-4 Adding a VoiceMail Service (Continued)



Click Add to finish adding the VoiceMail service.

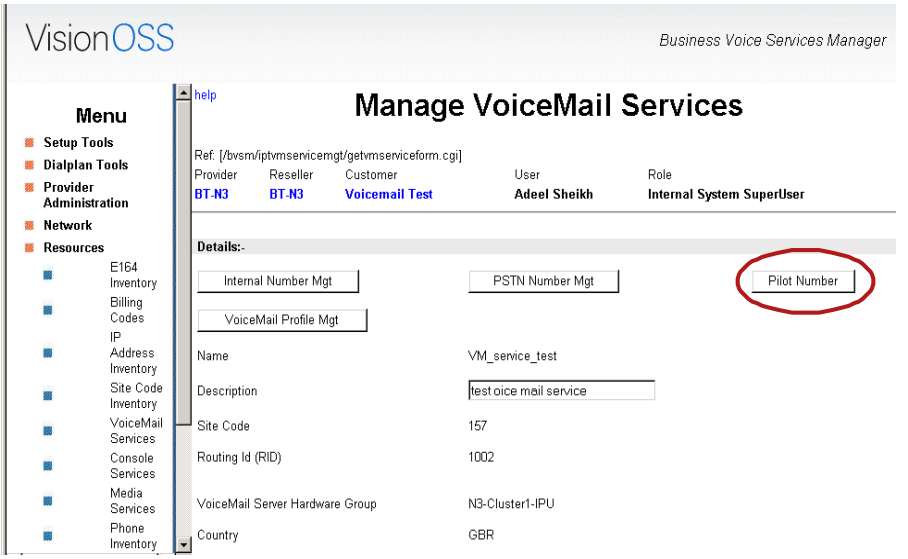
Adding Voicemail Pilot

To add a VoiceMail Pilot, use the following procedure:

Procedure

Step 1 Click the **Pilot Number** Button.

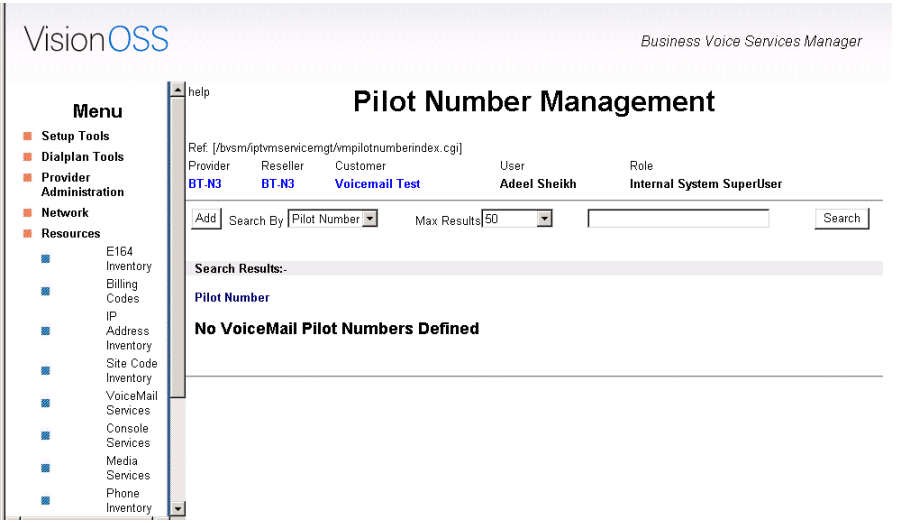
Figure 6-5 Adding Voicemail Pilot



The Pilot Number Management page displays.

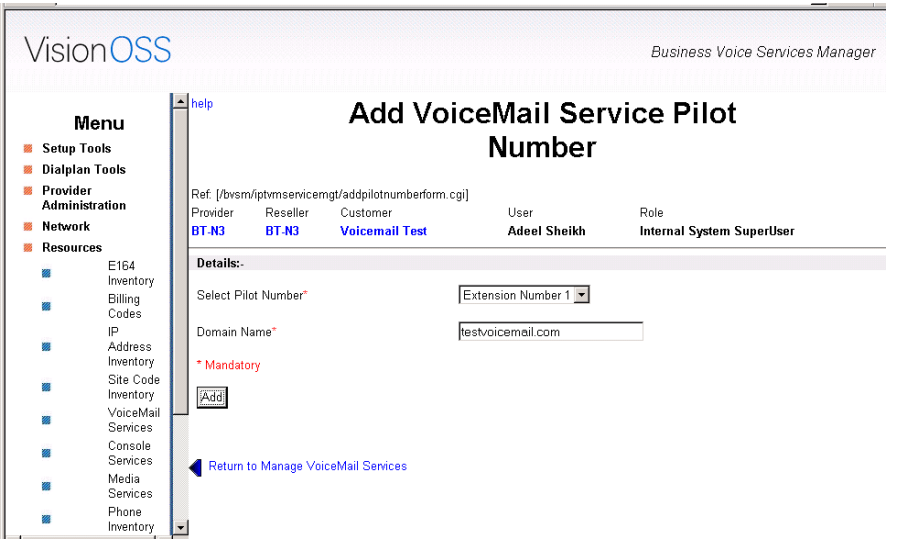
Step 2 Click the **Add** button to create a Pilot number.

Figure 6-6 Adding VoiceMail Pilot (continued)



Step 3 Select the Pilot number from the drop-down down list box, and click **Add**.

Figure 6-7 Adding VoiceMail Service Pilot Number



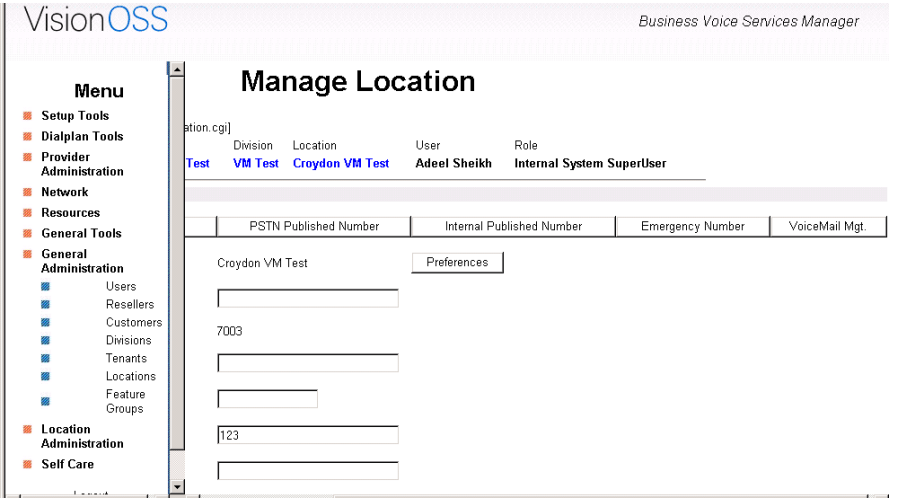
Adding a Voicemail Service for a Location

To add a VoiceMail service for a location, use the followin procedure:

Procedure

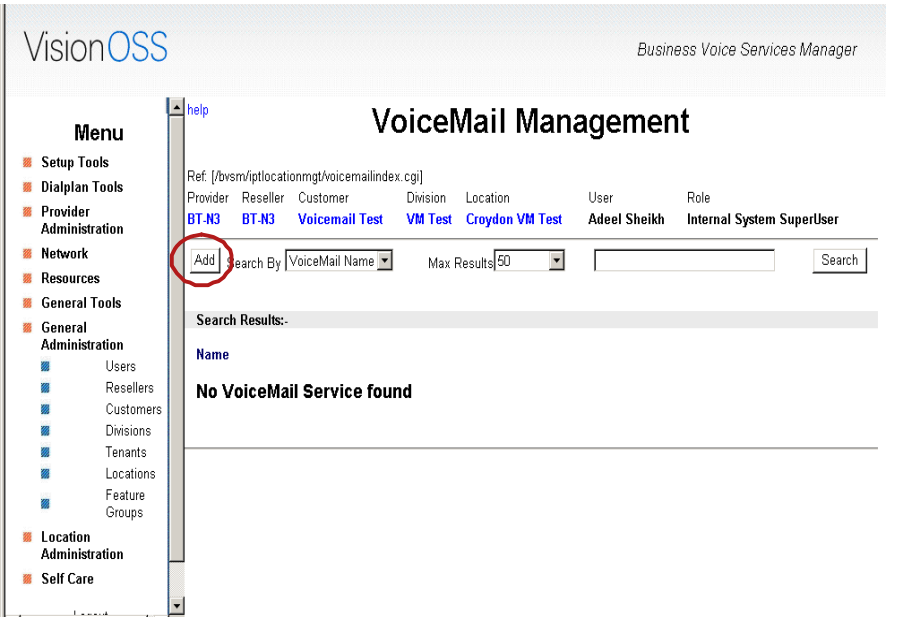
Step 1 Navigate to the Location and click VoiceMail Management.

Figure 6-8 Adding a VoiceMail Service for a Location



Click **Add** to create a VoiceMail service for that Location.

Figure 6-9 Adding a VoiceMail Service for a Location (continued)



Step 2 Provide the following details:

- Name: Enter a name for the VoiceMail Service.
- Select a VoiceMail Service: Select a VoiceMail servcie from the drop-down list box.

Step 3 Click **Add and Enable**.

Creating AutoAttendant Service

To create an AutoAttendant service, use the following procedure.

Procedure

Step 1 Navigate to Resources and click on **Auto Attendant Service**.

Step 2 The AutoAttendant screen displays; click **Add**.

Figure 6-10 Adding AutoAttendant Service

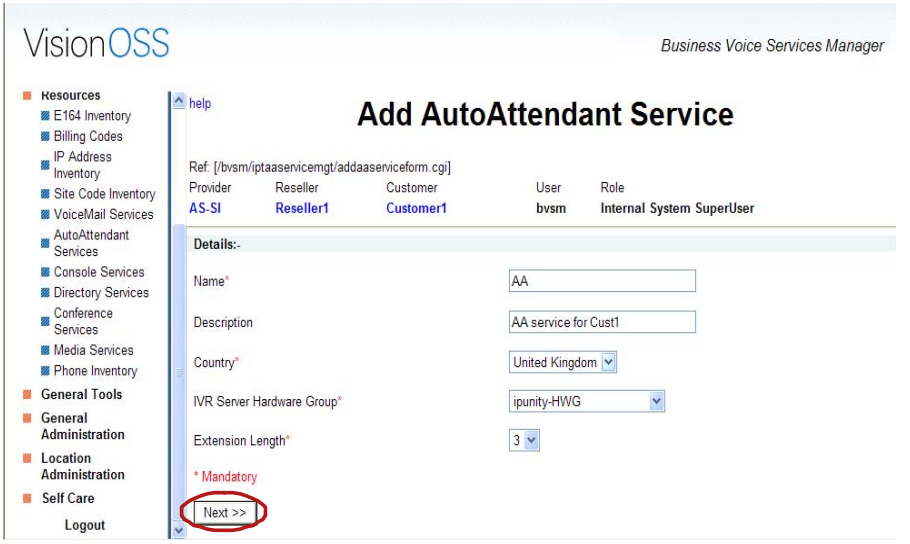
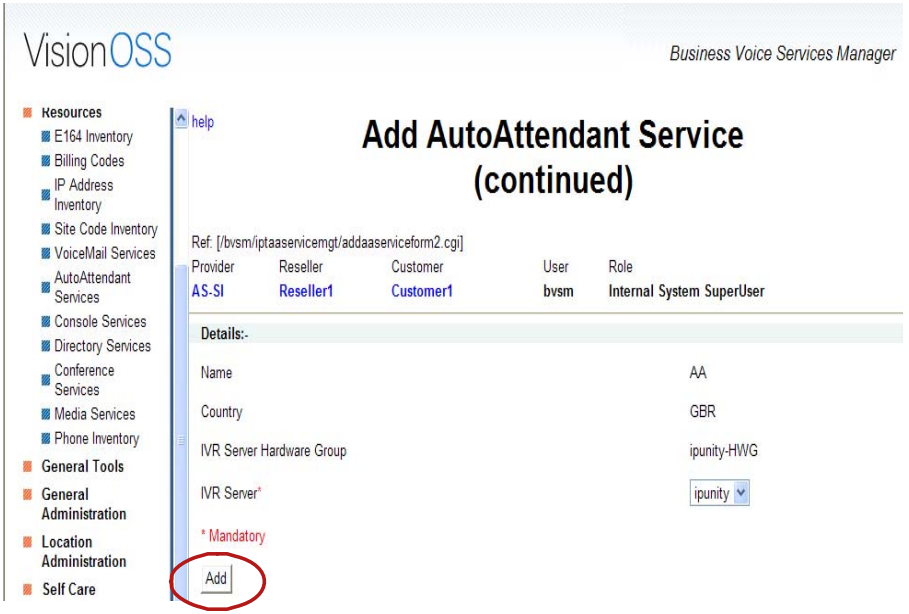
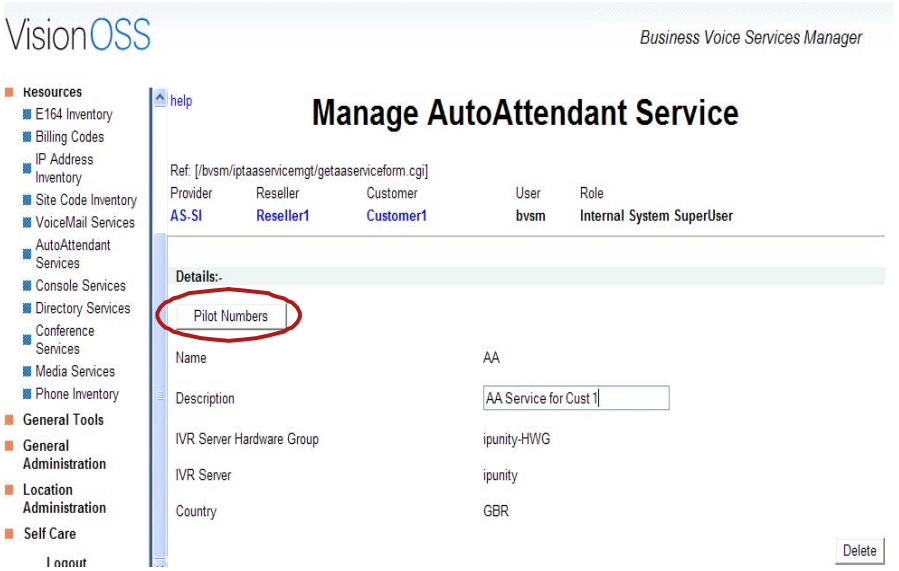


Figure 6-11 Adding AutoAttendant Service (continued)



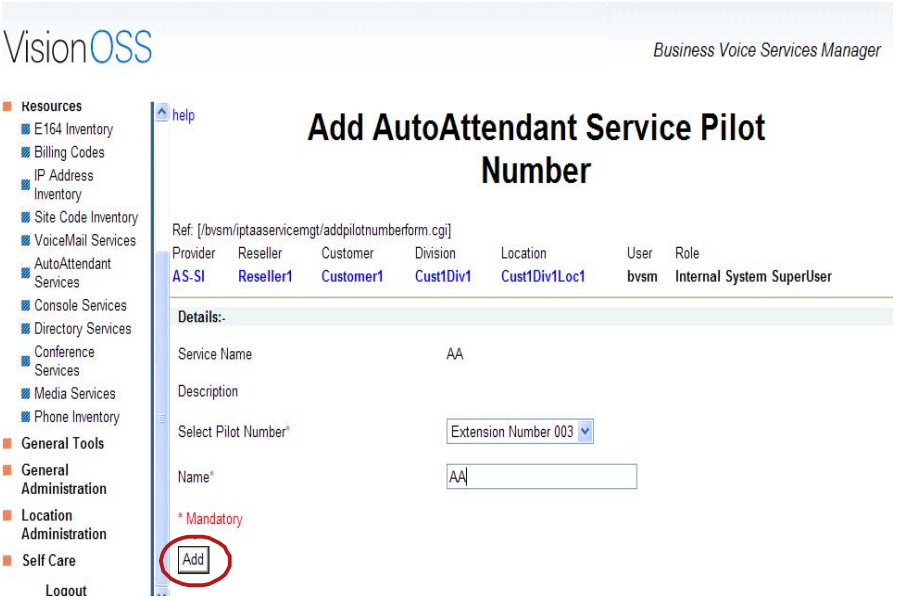
Step 3 Click Pilot Numbers to add the AutoAttendant Pilot.

Figure 6-12 Adding AutoAttendant Service (continued)



Step 4 Select the Pilot Number for the AutoAttendant from the drop down menu and click **Add**.

Figure 6-13 Adding AutoAttendant Service (continued)



Mapping E164 Number to an AutoAttendant Pilot Number

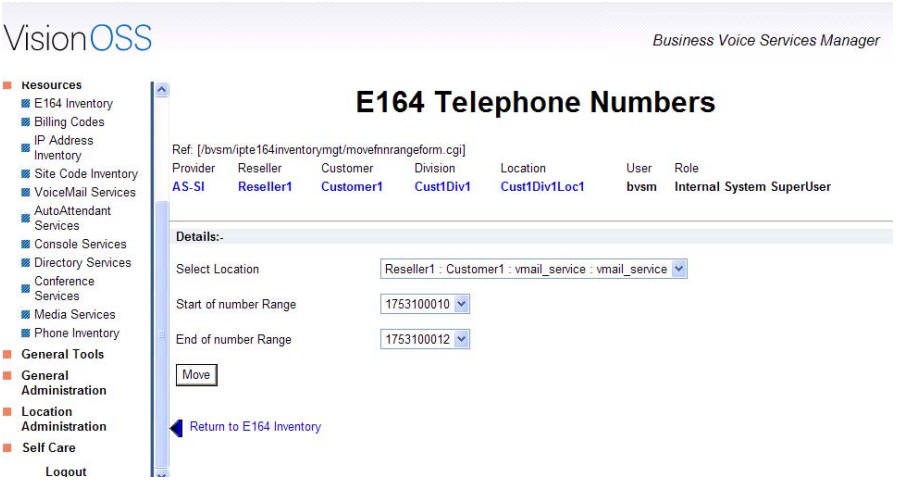
To associate E164 numbers to AutoAttendant pilot numbers, use the following procedure:

Procedure

Step 1 Move the E164 number range from provider level to the VoiceMail location.

Step 2 Map the numbers by going to PSTN Number Management and associating it with internal number (pilot number).

Figure 6-14 Mapping E164 Number



Configuring Movius Web Interface for Auto Attendant

After the AutoAttendant service and the pilot number have been configured on the BVSM, you must configure Movius web interface for AutoAttendant.

Before You Begin

1. Click on the configure IVR link appearing next to the pilot number. The Movius web interface displays.
2. It fetches the IP address of the AutoAttendant / IVR server from the network Tab configured in the BVSM.

Carry out the following procdeures to configure an AutoAttendant service:

Creating AutoAttendant Service

Procedure

Step 1 Log into the Movius Web interface as a system administrator.

Step 2 Once logged in, select the appropriate organization. In this case, the organization is 'Voicemail Service'.

Step 3 To log into the organization, click the log in link.

Step 4 Click **OK** when you are prompted to confirm that you really want to login and configure organization.

Step 5 Select AutoAttendant on left menu.

Step 6 Click the **Add** button.

Step 7 Add the AutoAttendant name (for example, e3AAServiceCust1)

Step 8 On AutoAttendant Phone Number, write the FINT number of the pilot (for example, 03210004999038)

Step 9 Select the phone type from the Phone Type drop-down list box.

Step 10 Select the transfer type from the Transfer Type drop-down list box.

Step 11 Click **Save** to create the AutoAttendant.

Creating Announcements

Use the following procedure to create specific announcements.

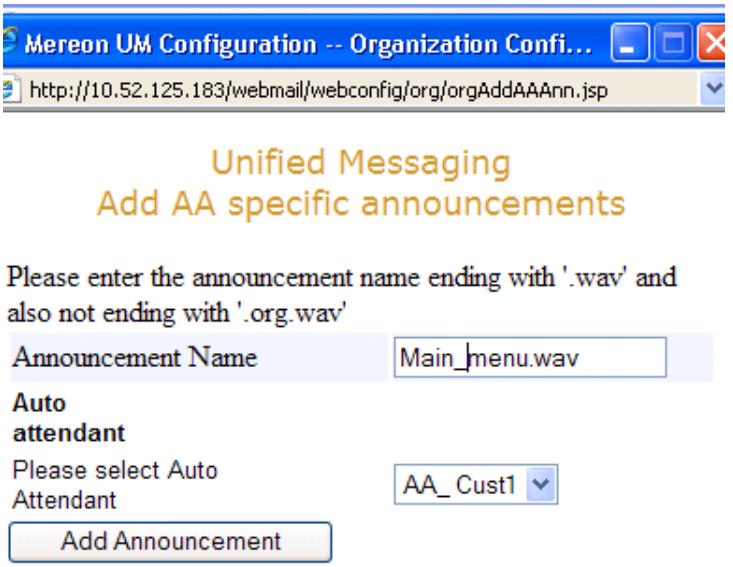
Procedure

Step 1 Click on the **Announcement Management** link.

Step 2 Click on **Add Specific Announcement** to create an announcement.

Step 3 Make sure that the name ends with '.wav' extension.

Figure 6-15 Adding Specific Announcements



Step 4 Click the **Upload** link to upload the Audio File. This will pop up a message window.

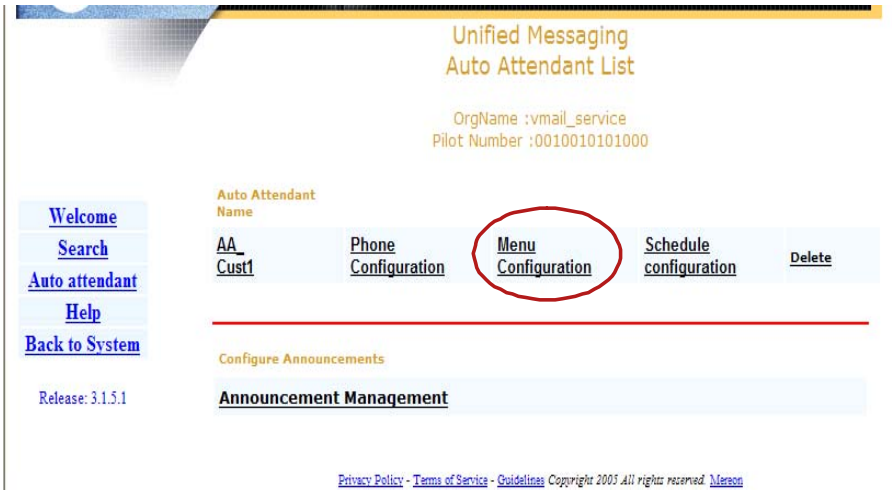
Menu Configuration

Use the following procedure to configure the AutoAttendant menu.

Procedure

Step 1 Click on the **Menu Configuration** option in the main AutoAttendant screen.

Figure 6-16 Configuring the AutoAttendant Menu



Step 2 Click **Add Menu** to create a menu for your AutoAttendant.

Step 3 Click on the menu name to display the configuration screen.

Step 4 Click the **Add** button to select an action against a specific key.

AutoAttendant Schedule

Use the follwoin procdedure to edit the AutoAttendant schedule.

Procedure

Step 1 Click **Edit** to change the timings or the menu.

Step 2 Make the appropriate changes.

Step 3 Click **Save**.

Configuring AutoAttendant Mapping Key

Use the followin steps to configure AutoAttendant Mappin Key:

Procdedure

Step 1 Log in as ipunity user in the OAM pag.e You can find it at

http://<hostname>/oam.

Step 2 Choose **Configuration > Framework Configuration > Framework**.

Step 3 Choose **Application Parameters > ipunity.apps.vm.UMApp > ipunity.apps.vm.AutoAttendantCall > FSM keys**.

Click on the FSM Key and Click **Add**. Make sure you have the correct pilot number that you have configured for your AutoAttendant.

AutoAttendant Media Termination Point Configuration on Cisco Unified Communications Manager Cluster

This section describes how to configure Media Termination Points (MTPs) on VoiceMail tTrunk. A Media Termination Point is required in the VoiceMail trunk on all the Unified CM clusters.

Use the following procedure to configure MTPs:

Procedure

Step 1 Log into Cisco Unified Communications Manager Administration of all the Unified CM clusters on the Hosted UCS platform. This can be accessed via:

https://<Unified_CM-Publisher_IP_Address>/ccmadmin

Step 2 For Unified CM 5.x and 6.x, go to **Device > Trunk**.

Step 3 Select the VoiceMail trunk. The name is <Unified_CM_cluster_name>-Vmail (for example, e3c5-Vmail).

Step 4 Check the **Media Termination Point Required** checkbox.

Step 5 Click Save to save your changes.

CHAPTER 7

Provisioning the Local PSTN Breakout Support

This chapter details how Public Switched Telephone Network (PSTN) calls can be routed via Local Gateways in the Hosted UCS reference architecture for Hosted UCS 6.1(a). It also provides steps required to provision the Local PSTN Breakout feature via the VisionOSS BVSM application.

In Hosted UCS 6.1(a), the administrator can provision local gateways with or without SRST support. Calls to/from PSTN can be routed via PRI or BRI interfaces. The format of the Calling and Called party number and Nature of Addres (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 or International calls.

This chapter is divided into the following sections:

- Introducing Local PSTN Breakout Support, page 7-1
- Provising Local PSTN Breakout Support, page 7-6

Introducing Local PSTN Breakout Support

This section describes the key characteristics of the Local PSTN Breakout Support feature:

- Handling PSTN Calls via Central Gateway, page 7-2
- Handling PSTN Calls via Local Gateway, page 7-4

- Support for Multiple Trunk Types for Local PSTN Breakout, page 7-5
- Support for Multiple Local Gateway Interfaces, page 7-5
- Support for Cisco Unified SRST, page 7-6

Handling PSTN Calls via Central Gateway

In Cisco Hosted Unified Communications Services 6.1(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
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

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

Table 7-4 Incoming calls from PSTN via Central Gateway in the United States

Call Type	cgpn (A)	ANOA	cdpn (B)	BNOA
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).

Handling PSTN Calls via Local Gateway

In Cisco Hosted Unified Communications Services 6.1(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.

In countries where there is no distinction between national and local dialing (for example Denmark, Qatar, and so on) Local Gateway trunks can be configured for

- No Local Dialing—This will result in all non-international calls being treated as national calls.

In countries where there is a distinction between national and local dialing (for example UK, Germany, and so on) 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.
- Local Dialing without Area Code—This will result in local calls presented to the PSTN without the NDC.

In the US, there is a distinction between national dialing, local dialing with the NPA (10-digit dialing) and local dialing without the NPA (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 NPA.
- Local Dialing without Area Code—This will result in local calls presented to the PSTN without the NPA.

Additionally, for all countries, the Local Gateway trunks can be configured to set the Called Party Number (cdpn) B and the cdpn Nature of Address (BNOA) as

NOA—In this case the cdpn is set in a relevant format together with appropriate NOA based on the called destination;

NoNOA—In this case the NOA is set to Unknown and the cdpn is prefixed with appropriate leading digits to distinguish called destinations.

Support for Multiple Trunk Types for Local PSTN Breakout

In Cisco Hosted Unified Communications Services 6.1(a), you can associate a location to one or two local gateway trunks:

- If a location is connected to one local gateway trunk, all PSTN calls would be routed via that trunk.
- If a location is connected to two local gateway trunks, the first trunk, connected to a long-distance provider, would be used to route National and International calls, and the second trunk, connected to the local exchange carrier (LEC), would be used to route local calls. In Hosted UCS 6.1(a), this is known as a **Local Override** option.

Support for Multiple Local Gateway Interfaces

In Cisco Hosted Unified Communications Services 6.1(a), Local Gateways can route calls via:

- PRI interfaces
- BRI interfaces

Support for Cisco Unified SRST

Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) provides Unified CM with fallback support for Cisco IP phones that are attached to a Cisco router on the local network. Cisco Unified SRST enables routers to provide call-handling support for Cisco IP phones when they lose connection to remote primary, secondary, or tertiary Unified CM installations or when the WAN connection is down.

In Cisco Hosted Unified Communications Services 6.1(a), you can associate a location to Local Gateway for Local PSTN Breakout with or without SRST support.

Most provisioning steps for Local PSTN Breakout support are common for Local Gateways with and without SRST support, and any SRST specific configuration steps are also provided.

Provising Local PSTN Breakout Support

This section describes required steps to provision Local PSTN Breakout support using Local Gateways:

- Static Configuration, page 7-6
- Loading the IOS Model, page 7-15
- Defining IOS Devices, page 7-16
- Initiating Local PSTN Breakout Support, page 7-20
- Adding and Configuring Local Gateways, page 7-21

Static Configuration

This section details the initial static (manual) configuration required for Local PSTN breakout support of the following Hosted UCS components:

- Cisco PGW Static Configuration, page 7-7
- Cisco Off-Net HSI Static Configuration, page 7-9
- Cisco Gatekeeper Static Configuration, page 7-10

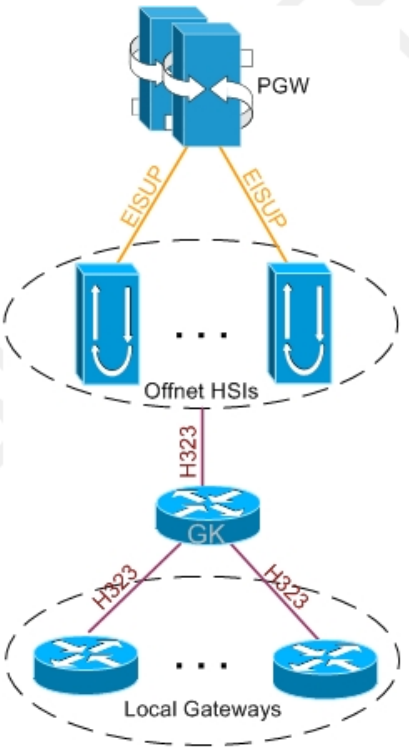
- Local Gateway Static Configuration, page 7-11

Cisco PGW Static Configuration

This section describes the required setup on the Cisco PGW before provisioning Local PSTN Breakout support.

In Hosted UCS 6.1(a), one or more dedicated off-net HSIs are required to provide the H.323 trunks between the PGW and local gateways that will be used for local PSTN breakout. The interface between the PGW and HSIs is an EISUP trunk, as shown in Figure 1

Figure 7-1 PGW/HSI/Local Gateway Interfaces



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

```
prov-add:EXTNODE:NAME="hsi-ent4of1",DESC="City 4 offnet HSI
1",TYPE="H323",ISDNSIGTYPE="N/A",GROUP=0
prov-add:EISUPPATH:NAME="eisup-hsi-ent4of1",DESC="Eisuppath signaling
service for
HSI-ENT4OF1",EXTNODE="hsi-ent4of1",CUSTGRPID="ILGW",ORIGLABEL="",TERML
ABEL=""
prov-add:IPLNK:NAME="iplnk-hsi-ent4of1",DESC="Iplnk for
HSI-ENT4OF1",SVC="eisup-hsi-ent4of1",IPADDR="IP_Addr1",PORT=8003,PEERA
DDR="10.120.4.33",PEERPORT=8003,PRI=1,IPROUTE=""
```

Note For detailed information, refer to the C*isco Media Gateway Controller Software Release 9 Provisioning Guide*

The following attributes need to be provisioned on the PGW:

- Trunk Group for each HSI. To add a trunk group, use—prov-add:trnkgrp:name="<trnkgrp_name>",clli="<clli_name>",svc="<signaling_svc>",type="<type>",selseq="<selseq>",qable="<qable>", for example:

  ```
  prov-add:trnkgrp:name="1101",clli="hsi-ent4of1",svc="eisup-hsi-ent
  4of1",type="IP",selseq="LIDL",qable="n"
  ```

- Routing Trunk Group for each off-net HSI. To add the routing trunk group, use—prov-add:rttrnkgrp:name="<rttrnkgrp_name>",type=4,reattempts=0,queuing=0,cutthrough=3,resincperc=0, for example:

  ```
  prov-add:rttrnkgrp:name="1101",type=4,reattempts=0,queuing=0,cutth
  rough=3,resincperc=0
  ```

Note Repeat this step for each HSI.

- Route to the HSI. To add the route, use—prov-add:rttrnk:weightedTG="OFF",name="route2offnethsi",trnkgrpnum=<rttrnkgrp_name>, for example:

  ```
  prov-add:rttrnk:weightedTG="OFF",name="route2offnethsi",trnkgrpnum
  =1101
  ```

- To associate routing trunk groups for the remaining HSIs to the "route2offnethsi" route, add the following for each remaining HSI—prov-ed:rttrnk:name="route2offnethsi",trnkgrpnum=<rttrnkgrp_name>, for example:

  ```
  prov-ed:rttrnk:name="route2offnethsi",trnkgrpnum=1102
  ```

- Route List to the HSI. To add the route list, use—prov-add:rtlist:name="rtlist2offnethsi",rtname="route2offnethsi",distrib="OFF"
- You must at least provision the following HSI Trunk Group Properties—"CustGrpId", "AllowH323Hairpin", and "GatewayRBToneSupport". To add the trunk group properties, use—prov-add:trnkgrpprop:name="<rttrnkgrp_name>",custgrpid="ILGW", AllowH323Hairpin="1",GatewayRBToneSupport="1", for example:

  ```
  prov-add:trnkgrpprop:name="1101",custgrpid="ILGW",AllowH323Hairpin
  ="1",GatewayRBToneSupport="1"
  ```

Note Repeat this step for each HSI

Cisco Off-Net HSI Static Configuration

The Off-Net HSI enables the Cisco PGW to talk to the Local Gateways using H.323 via the H.323 gatekeeper. The HSI is an adjunct to the Cisco PGW and simply provides an H.323 interface.

Apart from the configuration described in this section, Cisco HSI has mandatory parameters that need to be provisioned; for example, IP Addresses of the HSI and the PGWs, Ports used to communicate with the PGW.

Note For further information, refer to the Cisco H.323 Signaling Interface User Guide, Release 4.2.

Configure the following HUCS specific static configuration settings on all Off-Net HSIs:

- RAS Parameters
  - prov-add:name=ras,gatekeeperId=**HUCS_OFFNET_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-ent4of1@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

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), Unified CM, and any H.323 customer devices such as the Local Gateways. The gatekeeper forces all routing to use the Cisco PGW.

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

- gatekeeper
- zone local HUCS_OFFNET_ZONE cisco.com

Local Gateway Static Configuration

At the least, Local Gateways should be configured to enable BVSM to communicate with it.

Following is an example basic configuration on a 3845 ISR, with:

- 1 x NM-HDV2 with 1 x VWIC-2MFT-E1-DI;
- 1 x NM-HDV2-2T1/E1 with 1 x VWIC-2MFT-E1-DI;
- 1 x NM-HD-2VE with 1 x VIC2-2FXO and 1 x VIC2-4FXO;
- 1 x NM-HD-2VE with 2 x VIC2-2BRI-NT/TE

```
e4lgw1#sh ver
Cisco IOS Software, 3800 Software (C3845-IPVOICEK9-M), Version
12.4(15)T7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Jan-08 00:11 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

e4lgw1 uptime is 2 weeks, 1 day, 22 hours, 51 minutes
System returned to ROM by power-on
System restarted at 15:08:12 GMT Wed Jan 7 2009
System image file is "flash:c3845-ipvoicek9-mz.124-15.T7.bin"
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.


Cisco 3845 (revision 1.0) with 218112K/44032K bytes of memory.
Processor board ID FCZ113872WL
2 Gigabit Ethernet interfaces
31 Serial interfaces
4 ISDN Basic Rate interfaces
6 Channelized E1/PRI ports
```

```
6 Voice FXO interfaces
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
e4lgw1#sh run
Building configuration...

Current configuration : 1306 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname e4lgw1
!
boot-start-marker
boot system flash:c3845-ipvoicek9-mz.124-15.T7.bin
boot-end-marker
!
card type e1 2 1
enable secret 5 $1$7dKw$5IGznKUAfZdiL.PRKBTmg1
!
no aaa new-model
clock timezone GMT 0
clock summer-time BST recurring last Sun Mar 2:00 last Sun Oct 2:00
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate slot 3
no network-clock-participate slot 4
ip cef
!
no ip domain lookup
ip domain name ipcbuemea.cisco.com
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
!
voice-card 2
 no dspfarm
!
voice-card 3
 dspfarm
```

```
!
voice-card 4
 no dspfarm
!
controller E1 1/0/0
!
controller E1 1/0/1
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/0/0
!
controller E1 2/0/1
!
interface GigabitEthernet0/0
 ip address 10.190.4.111 255.255.255.0
 duplex full
 speed 100
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.191.4.111 255.255.255.0
 duplex full
 speed 100
 media-type rj45
!
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
no ip http secure-server
!
control-plane
!
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
```

```
!
scheduler allocate 20000 1000
ntp server 10.100.100.2
ntp server 10.100.100.3
!
end
```

Furthermore, in Hosted UCS 6.1(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, for example to the ATS (10.100.100.2), which contains the Hosted UCS 6.1(a) TCL applications, for example hucstrans_v0.1-5.tar. Currently, the tar files are stored on the ATS in /tftpboot/LocalGatewayTCL.

Step 2 On the Voice Gateway, execute the following command in priviledged EXEC mode:

<hostname>**#archive tar /xtract (t)ftp://<host>/<file.tar> flash:**; for example:

```
e4lgw1#archive tar /xtract
tftp://10.100.100.2/LocalGatewayTCL/hucstrans_v1.0-5.tar flash:
```

You should see a similar output:

```
Loading LocalGatewayTCL/hucstrans_v1.0-5.tar from 10.100.100.2 (via
GigabitEthernet0/0): !
extracting hucstrans-readme.txt (1161 bytes)
extracting hucstrans.tcl (14469 bytes)
extracting hucstransfallback.tcl (20959 bytes)
[OK - 36589 bytes]
```

Step 3 Verify that the TCl applications have been stored in flash:

```
show flash:
-#- --length-- -----date/time------ path
…
```

```
9     41824688 Dec 18 2008 11:36:56 +00:00
c3845-ipvoicek9-mz.124-15.T7.bin
10   14469 Jan 14 2009 16:28:42 +01:00  hucstrans.tcl
11   20959 Jan 14 2009 16:28:40 +01:00  hucstransfallback.tcl
13   1161  Jan 14 2009 16:28:38 +01:00  hucstrans-readme.txt
```

If the Local Gateway is already configured and you are upgrading the TCL application, you need to reload the voice application scripts. To reload the voice application scripts after they have been modified execute the following commands in priviledged EXEC mode:

- e4lgw1#call application voice load hucstrans
- e4lgw1#call application voice load hucstransfallback

Repeat this procedure for all Local Gateways.

Loading the IOS Model

This section describes required steps to load the Hosted UCS 6.1(a) IOS model. This model defines how BVSM should configure the Local Gateways.

To prepare BVSM by loading the 'IOSDevice_12_x' IOS Model, use the following procedure:

Procedure

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

Step 2 Click **Load IOSDevice Models**.

Step 3 Browse for the model loader being used, and click **Upload file**.

Note Check for any errors or warnings once the loading completes.

Defining IOS Devices

In the Hosted UCS environment for local PSTN breakout support, BVSM needs the information about the type of media gateways used in order to provision the Local Gateways. BVSM administrator defines an IOS Device (Type, Network Modules and Interface Cards). This information is later used to add and configure the Local Gateways. The following sections describe how IOS Device components are defined:

- Add IOS Device Types, page 7-16
- Add IOS Device Network Modules, page 7-17
- Adding IOS Device Interface Cards, page 7-19

Caution Ensure that you are Adding IOS Device Components to the correct Provider.

Note To get to the Provider level, choose **Provider Administration > Providers**, and select a Provider

Add IOS Device Types

To add an IOS Device Type:

Step 1 Choose Setup Tools>Vendor Tools.

Step 2 Click **IOS Device**

Step 3 Click **IOS Device Types**

Step 4 Click **Add**.

Step 5 Under **Details**, enter the following :

- Name: <uniquename>; for example, C3845
- Description: <IOSDeviceTypeDesc>; for example, Cisco 3845
- IOS Device Type (as referred to by CallManager): <IOSCUCM>; for example, C3845
- IOS Device Type (as referred to by PGW): <IOSPGW>; for example, **C3845**

- Type: <IOSorNonISR>; for example, **ISR**

Step 6 Under Fixed Ports, enter the following:

- Number of Ethernet Ports: <EthPorts>, for example 0
- First Ethernet Port Number: <FirstEthPort>, for example 0
- Number of FastEthernet Ports: <FastEthPorts>, for example 0
- First FastEthernet Port Number: <FirstFasEthPort>, for example 0
- Number of GigabitEthernet Ports: <GigEthPorts>, for example 2
- First GigabitEthernet Port Number: <FirstGigEthPort>, for example 0
- Number of E1 WAN Ports: <E1Ports>, for example 0
- First E1 WAN Port Number: <FirstE1Port>, for example 0
- Number of T1 WAN Ports: <T1Ports>, for example 0
- First T1 WAN Port Number: <FirstT1Port>, for example 0
- Number of Analogue Ports: <AnPorts>, for example 0
- First Analogue Port Number: <FirstAnPort>, for example 0

Step 7 Under 'Network Module Slots', enter the following:

- Number of Network Modules Supported: <NMs>, for example 4
- First Network Module Slot Number: <FirstNMSlot>, for example 1

Step 8 Click **Add**.

Note Repeat this for all IOS Device Types.

This procedure updates BVSM.

Add IOS Device Network Modules

To add an IOS Device Network Module, use the following procedure:

Procedure

Step 1 Go to Setup Tools>Vendor Tools.

Step 2 Click "IOS Device"

Step 3 Click "IOS Device Network Modules"

Step 4 Click "Add"

Step 5 Under 'Details', enter the following:

- Name: <uniquename>; for example, **NM-HDV2-ISR**
- Description: <IOSDeviceNMDesc>; for example, **NM-HDV for ISR**

Step 6 Under 'Fixed Ports', enter the following:

- Number of Ethernet Ports: <EthPorts>, for example 0
- First Ethernet Port Number: <FirstEthPort>, for example 0
- Number of FastEthernet Ports: <FastEthPorts>, for example 0
- First FastEthernet Port Number: <FirstFasEthPort>, for example 0
- Number of GigabitEthernet Ports: <GigEthPorts>, for example 0
- First GigabitEthernet Port Number: <FirstGigEthPort>, for example 0
- Number of E1 WAN Ports: <E1Ports>, for example 0
- First E1 WAN Port Number: <FirstE1Port>, for example 0
- Number of T1 WAN Ports: <T1Ports>, for example 0
- First T1 WAN Port Number: <FirstT1Port>, for example 0
- Number of Analogue Ports: <AnPorts>, for example 0
- First Analogue Port Number: <FirstAnPort>, for example 0

Step 7 Under 'Interface Card Slots', enter the following:

- Number of Slots: <ICs>, for example 1
- First Slot Number: <FirstICSlot>, for example 0
- Interface Card Port Number Format: <ICPortNumberFormat>, for example module/slot/port

Step 8 Click **Add**.

Note Repeat this procedure for all IOS Device Network Modules.

This procedure updates BVSM.

Adding IOS Device Interface Cards

To add an IOS Device Interface Card, use the following steps:

Procedure

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

Step 2 Click **IOS Device**.

Step 3 Click **IOS Device Interface Cards**.

Step 4 Click **Add**.

Step 5 Under Details, enter the following:

- Name: <uniquename>; for example, VWIC-2MFT-E1-DI
- Description: <IOSDeviceICDesc>; for example, VWIC-2MFT-E1-DI

Step 6 Under Ports, enter the following:

- Number of Ethernet Ports: <EthPorts>; for example, 0
- First Ethernet Port Number: <FirstEthPort>; for example, 0
- Number of FastEthernet Ports: <FastEthPorts>; for example, 0
- First FastEthernet Port Number: <FirstFasEthPort>; for example, 0
- Number of GigabitEthernet Ports: <GigEthPorts>; for example, 0
- First GigabitEthernet Port Number: <FirstGigEthPort>; for example, 0
- Number of E1 WAN Ports: <E1Ports>; for example, 2
- First E1 WAN Port Number: <FirstE1Port>, for example 0
- Number of T1 WAN Ports: <T1Ports>; for example, 0
- First T1 WAN Port Number: <FirstT1Port>; for example, 0

- Number of Analogue Ports: <AnPorts>; for example, 0
- First Analogue Port Number: <FirstAnPort>; for example, 0

Step 7 Click **Add**.

Note Repeat this for all IOS Device Interface Cards

This procedure updates BVSM.

Initiating Local PSTN Breakout Support

Support for Local PSTN Breakout must be initialized on the PGW. To initialize the PGW,use the following steps:

Procedure

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

Step 2 Select the PGW you want to initialize.

Step 3 Click **Prepare for Local Gateway**.

Note Repeat this for all PGWs.

This procedure updates BVSM and PGW.

Adding and Configuring Local Gateways

There are several steps required to define and configure Local Gateways with or without SRST. Most steps are common for Local Gateways with and without SRST support. Section 3.1.5.3 includes SRST specific configuration required for Local Gateways with SRST support. The administrator needs to:

Define Local Gateways, page 7-21

Define Local Gateways

A Local Gateway is defined in BVSM as a Generic Cisco IOSDevice. To define a Local Gateway, use the following steps:

Procedure

Step 1 Choose **Network > Gateways**.

Step 2 Click **Add**.

Step 3 Click **Add** next to IOSDevice (Generic Cisco IOSDevice)

Step 4 Under Details, enter the following:

- Host Name: <uniquename>, same as the local gateway hostname; for example, e4lgw1
- Description: <localgatewaydescription>; for example, City 4 Local Gateway 1
- Country: <CountrywhereGatewayis>, for example United States
- Device Type: <DeviceType>; for example, C3845

Step 5 Under 'Connectivity Details', enter the following:

- IP Address: <gatewayIP>; for example, 10.190.4.111
- Alternate IP Address: <gatewayIP2>; for example, 10.191.4.111
- Config Password: <configpassword>; for example, cisco
- Enable Password: <enablepassword>; for example, cisco
- Version: <gatewayIOSversion>; for example, IOSDevice : 12.x
- Select **Detailed trace file of configuration sessions ?**

Step 6 Under Roles, enter the following:

- Tick the 'IP PBX' box
- IPPBX lines: <IPPBXlines>, for example: 1000
- Tick the 'PSTN Gateway' box
- PSTN lines: <PSTNlines>, for example: 1000

Step 7 Click **Add**.

Note Repeat this for all required Media Gateways.

This procedure updates BVSM only.

Associate Local Gateways with Gatekeepers

To associate Local Gateways with a Gatekeeper, use the following steps:

Procedure

Step 1 Choose Network>Gateways

Step 2 Click **Connectivity** next to the gateway you want to associate; for example, e4lgw1

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

Step 4 Select the Gatekeeper you want to connect the local gateway to; for example, GK2600-ENT4A

Step 5 Click **Connect**.

Note Repeat this for all required Local Gateways.

This procedure updates BVSM only.

Configure SRST

Note This procedure is required only for Local Gateways with SRST support.

To configure SRST, use the following steps:

Procedure

Step 1 Go to **Network > Gateways**.

Step 2 Select the gateway you want to configure, and click **SRST Config**.

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

- SRST IP Address: <GatewayIP>, IP address of the relevant Local Gateway interface used to configure the Cisco Unified CM fallback; for example, 10.190.4.111.
- Max. Phone supported in SRST mode <max-ephones>; for example, 32
- Max. Lines supported in SRST mode <max-dn>; for example, 32

Step 4 Click **Apply**.

Note Repeat this for all required Local Gateways.

This procedure updates BVSM only.

Note BVSM cannot provision a SRST reference in Cisco Unified CM, due to AXL API limitations. You must configure the SRST reference on all Unified CM servers that have the locations which use this Local Gateway.

A survivable remote site telephony (SRST) reference comprises the gateway that can provide limited Unified CM functionality when all other Unified CM servers for a device are unreachable. Typically assigned to device pools, SRST references determine the gateways where calling devices search when they attempt to complete a call if Unified CM is unavailable.

To configure the SRST reference in Unified CM, use the following steps:

Procedure

Step 1 Choose **System > SRST**.

Step 2 Click **Add New** and use the following settings:

- For Unified CM 4.2(3)
  - SRST Reference Name: <GatewayIP>, IP address of the relevant Local Gateway interface used to configure the Cisco Unified CM fallback; for example, 10.190.4.111
  - IP Address: <GatewayIP>; for example, 10.190.4.111
  - Port: <SRSTPort>; for example, 2000
  - SRST Certificate Provider Port: <SRSTCertProvPort>; for example, 244
  - Click **Insert**.
- For Unified CM 5.1(3) and 6.1(2)
  - Name: <GatewayIP>, IP address of the relevant Local Gateway interface used to configure the Cisco Unified CM fallback, for example 10.190.4.111
  - Port: <SRSTPort>; for example, 2000
  - IP Address: <GatewayIP>; for example, 10.190.4.111
  - SIP Port: <SIPPort>; for example, 5060
  - SRST Certificate Provider Port: <SRSTCertProvPort>; for example, 2445
  - Click **Save**.

Configure Local Gateway Protocol

In Hosted UCS 6.1(a), signalling between Local Gateways and PGWs/HSIs is carried out via H.323. To configure H.323 signalling, use the following steps:

Step 1 Go to **Network > Gateways**. Select the gateway you want to configure.

Step 2 Click **Gateway Config**.

Step 3 Select H.323 as the Gateway Protocol.

Step 4 Click **Next >>**.

Step 5 Under H323 : Details enter the following:

- H.323 Interface: <H323Interface>, for example FastEthernet0/0
- Switch Type: <GlobalConfigISDNSwitch-Type>, for example primary-net5

Step 6 Click **Apply**.

Note Repeat this for all required Media Gateways.

Note If the Gateway is configured in the US, an option to configure Local Dialing will be available. This option was required in Hosted UCS 5.1(b), but is not in Hosted UCS 6.1(a). Therefore any value can be configured for this field. Bugzilla 4158 has been raised to address this issue.

This procedure updates BVSM and Local Gateway.

Configure Network Modules used on the Local Gateway

To configure Network Modules used on the Local Gateway, use the following steps:

Procedure

Step 1 Choose **Network > Gateways** and select the gateway you want to configure.

Step 2 Click **Network Module Mgt**.

Step 3 Select the required Network Module in the correct Slot Number; for example, select NM-HDV2-NonISR in Slot Number 2.

Step 4 Click Update.

Note Repeat this for all required Network Modules and for all Media Gateways.

This procedure updates BVSM only.

Configure Interface cards used on the Local Gateway

To configure Interface Cards used on the Local Gateway, use the following steps:

Procedure

Step 1 Choose **Network > Gateways**. Select the gateway you want to configure.

Step 2 Click **Network Module Mgt**.

Step 3 Click Interface Cards.

Step 4 For each Device Slot, select the used Interface Card in the correct Slot Number; for example, for an NM-HDV2-NonISR in Device Slot 2 select VWIC-2MFT-E1-DI in Slot Number 0.

Step 5 Click **Update**.

Note Repeat this procedure for all required Interface Cards and for all Media Gateways.

This procedure updates BVSM only.

Define Local Gateway Interfaces

In Hosted UCS 6.1(a) Local Gateways can route calls via PRI interfaces and BRI interfaces.

Following sections describe how these interfaces can be configured:

Caution 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; you must define a Port used on the Local Gateway, and then define a trunk used on the previously defined port.

To define a Port used on the Local Gateway, use the following steps:

Procedure

Step 1 Choose **Network > Gateways**. Select the gateway you want to configure.

Step 2 Click **Port Management.**

Step 3 Click Configure next to the port you want to configure, for example Serial2/0 (E1)

Step 4 Under 'Port Configuration', enter the following:

- Codec Complexity: <CodecComplex>; for example, flex
- Framing: <Framing>; for example, no-crc4
- Line Code: <LineCode>; for example, hdb3
- Clock Source: <ClockSource>; for example, line
- DS0 Group: <DS0Group>; for example, 0

Step 5 Click **Apply**.

To define a Trunk used on the previously defined Port, use the following steps:

Procedure

Step 1 Go to **Network > Gateways**. Select the gateway you want to configure.

Step 2 Click **Port Management**.

Step 3 Click **Configure** next to the port you have configured in the previous step (the status of the port should be "Configured"); for example, Serial2/0/0 (E1)

Step 4 Click **Trunk Config**.

Step 5 Under Trunk Configuration, enter the following:

- Switch Type: <InterfaceConfigISDNSwitch-Type>, for example primary-net5

- Signalling Protocol: <SigProtocol>, PRI
- Use as: LocalGateway

Step 6 Click **Next >>**.

Step 7 Under Configuration, enter the following:

- PGW Name—<RelevantPGW>, for example PGW-ENT4
- Nature-of Address—<NOA>, If the expected format of the cdpn (B) and the BNOA is based on the called destination for Incoming/Outgoing PSTN calls via Local Gateways select NOA, and if the BNOA needs to be set to UNKNOWN with the corresponding cdpn (B) select NoNOA
- 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. For this select 10-digit local dialing.
- If this trunk is to be used for PSTN access when the phones are in SRST mode, tick the 'Primary PSTN Trunk' tick box.

Note Only one trunk can be set for each of these roles per Local Gateway. Additionally, this option will be available if SRST has been configured.

- If this trunk is to be used for Emergency access when the phones are in SRST mode, tick the 'Primary Emergency Trunk' tick box.

Click **Submit**.

Note Repeat this for all required PRI Interfaces and for all Local Gateways.

This procedure updates BVSM, PGW, and Local Gateway.

Define Local Gateway BRI Interface

To define a Port used on the Local Gateway, ue the following steps:

Procedure

Step 1 Choose **Network > Gateways**, and select the gateway you want to configure.

Step 2 Click "Port Management."

Step 3 Click "Configure" next to the port you want to configure, for example BRI4/0/0 (E1)

Step 4 Check that following detailsdisplay correctly:

- Host Name: <LocalGatewayName>; for example, e4lgw1
- Port Id: <port>; for example, BRI4/0/0
- Port Controller: <Protocol>; for example, BRI

Step 5 Click **Apply**.

To define a Trunk used on the previously defined Port, use the following steps:

Step 1 Go to **Network > Gateways**, and select the gateway you want to configure.

Step 2 Click **Port Management**.

Step 3 Click **Configure** next to the port you have configured in the previous step (the status of the port should be "Configured"); for example, BRI4/0/0 (E1)

Step 4 Click **Trunk Config**.

Step 5 Under Trunk Configuration, enter the following:

- Switch Type: <InterfaceConfigISDNSwitch-Type>, for example basic-net3
- Use as: LocalGateway

Step 6 Click **Next >>**.

Under Configuration, enter the following:

- PGW Name: <RelevantPGW>, for example PGW-ENT3

- Nature-of Address: <NOA>, If the expected format of the cdpn (B) and the BNOA is based on the called destination for Incoming/Outgoing PSTN calls via Local Gateways select NOA, and if the BNOA needs to be set to UNKNOWN with the corresponding cdpn (B) select NoNOA
- 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. For this select 10-digit local dialing.
- If this trunk is to be used for PSTN access when the phones are in SRST mode, select **Primary PSTN Trunk**.

Note This option is visible only if this is the first trunk on the E1.

- If this trunk is to be used for Emergency access when the phones are in SRST mode, select the Primary Emergency Trunk tick box This option is visible only if this is the first trunk on the E1.

Note This option is visible only if this is the first trunk on the E1.

Step 7 Click **Submit**.

Note Repeat this for all required BRI Interfaces and for all Local Gateways.

This procedure updates BVSM, PGW, and Local Gateway.

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 and connecting locations with Local Gateway trunk(s).

Before proceeding with the provisioning steps in this section ensure that

- PSTN Published Number has been added.
- Emergency Published Number has been added (if Cisco ER is not used).
- Overlay Area Codes have been defined (applicable for the US only).
- You haven't assigned any range of E164 numbers to internal numbers.

You can perform the following tasks under location administration:

Change Location Preferences, page 7-31

Connect Locations with Local Gateway Trunk(s), page 7-32

Assigning a Range of E164 Numbers to Internal Numbers, page 7-34

Caution Ensure that you are administering the correct Location; the name of the Location will be displayed on the screen.

Change Location Preferences

Two location preferences need to be changed so that the location can support local PSTN breakout. They are: 'AssociateFNNinRanges' and 'LocationCentralPSTNAccessOnly'. To change these location preferences:

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

Step 2 Select the location you want to configure.

Step 3 Click **Preferences**.

Step 4 Click **AssociateFNNinRanges**.

Step 5 Check the available checkbox to enable the setting.

Step 6 Click **Modify**.

Step 7 Click **Return to Preferences Management**.

Step 8 Click **LocationCentralPSTNAccessOnly**.

Step 9 Un-check the available checkbox to disable the setting.

Step 10 Click **Modify**.

Note Repeat this procedure for all required locations.

This procedure updates BVSM only.

Connect Locations with Local Gateway Trunk(s)

A location, depending on the requirements, can be associated to one or two local gateway trunks. If a location is connected to two local gateway trunks, the first trunk, connected to a long-distance provider, is used to route National and International calls, and the second trunk, connected to the local exchange carrier (LEC), is used to route local calls. In Hosted UCS 6.1(a), this is known as the **Local Override** option.

Use the follwoing steps to connect a location with one Local Gateway Trunk (No Local Override option):

Procedure

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

Step 2 Click **PSTN Connectivity**.

Step 3 Click **Next >>**.

Step 4 From the drop-down menu select the required gateway; for example, e4lgw1.

Step 5 Click **Next >>**.

Step 6 From the drop-down menu, select the required gateway port; for example, Serial2/1.

Caution If you select a local gateway trunk that is configured for "No Local Dialling", the screen gets updated to give you an option to configure the second local gateway trunk for the "Local Override" option. Make sure that you select 'None' From the drop-down menu.

Step 7 Click **Next >>**.

Step 8 Click **Submit**.

Use the following steps to connect a location with two Local Gateway Trunks (Local Override option):

Procedure

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

Step 2 Click **PSTN Connectivity**.

Step 3 Click **Next >>**.

Step 4 From the drop-down menu, select the required Gateway; for example, e4lgw1.

Step 5 Click **Next >>**.

Step 6 From the drop-down menu, select the required gateway port (this should be a local gateway trunk configured for No Local Dialling); for example, Serial2/0.

Step 7 Click **Next >>**.

Step 8 From the drop-down menu, select the required Local Override Gateway; for example, e4lgw1.

Step 9 Click **Next >>**.

Step 10 From the drop-down menu, select the required Local Override Gateway Port. This should be a local gateway trunk configured for "Local dialling without area code" or "10-digit local dialling"; for example, Serial2/1.

Step 11 Click **Next >>**.

Step 12 Click **Submit**.

Note Repeat this procedure for all required locations.

This procedure updates BVSM, PGW, and Ciso Unified Communications Manager.

Assigning a Range of E164 Numbers to Internal Numbers

For a range of internal extensions, the BVSM administrator can assign a range of E164 numbers. These can then be assigned to an IP Phone, so that users can receive calls from the PSTN on those extensions. For locations with Local PSTN breakout support, E164 numbers are associated with internal numbers by associating a range of 10n numbers, where n?{0,1,2,3,4}.

Note Make sure that the Location preference AssociateFNNinRanges has been enabled.

To assign a Range of E164 numbers to internal numbers using the in-ranges option, use the following steps:

Procedure

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

Step 2 Click **Range Assoc**.

Step 3 Under 'Select the Size of Range', enter the following:

- National Code: <NatCode>, select a national code, for example 212.
- Range Size: <RangeSize>, for example 10

Step 4 Click **Next >>**.

Step 5 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 6 Click **Submit**.

Note To associate a range of numbers not equal to 10n numbers, where n?{0,1,2,3,4}, Step 2 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 3 times (2x101 + 1x100).

Note You must repeat this procedure multiple times (if the range is not equal to 10n numbers, where n?{0,1,2,3,4}, as described in the previous note) and for all required locations.

This procedure updates BVSM, PGW, and local gateway.

Note Starting from Hosted UCS 6.1(a), BVSM 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. BVSM then invokes the HUCSprovx10 PGW script and inserts the associations into the PGW TimesTen database.

CHAPTER 8

Provisioning Netwise

This chapter describes the steps required to integrate a Netwise operator into the Cisco Hosted Unified Communications Services 5.1(b) platform. This requires the previous installation of the Netwise servers as described in the Netwise documentation. This chapter includes the following sections:

- Netwise Telephony Configuration Application Static Configuration, page 8-1
- Adding a Netwise Cluster to BVSM, page 8-2
- Configuring Operator Console Attributes, page 8-13
- Adding a Pilot Number, page 8-16
- Adding a Console Phone, page 8-18
- Managing Users, page 8-19
- Using Netwise Tools, page 8-19
- Standard Parameter Fields and Standard Layout, page 8-22

Netwise Telephony Configuration Application Static Configuration

To complete the static configuration on the Netwise telephony configuration application (TCA), perform the following steps:

Procedure

Step 1 To configure a new configuration to be used to provision the console, log into **http://***CMG Server IP Address***/TCA**.

Step 2 By default, the configuration name used by BVSM is *HUCS*, so create a new configuration from an empty template called **HUCS**.

Step 3 From the Host menu, add the various required hosts as follows:

- Publisher and subscribers of the cluster
- Netwise Contact Management (CMG) and Netwise CMG Telephony Server for Cisco Unified CM (CTC) servers in the Netwise cluster

Step 4 From the Telephony menu, create a new site; for example, called **HUCS**.

Step 5 From the new site, create a new Cisco Unified CM cluster, using all the hosts created before. The cluster must have the same name used on BVSM for the Cisco Unified CM cluster you want to install. To do this, complete the following steps:

a. From the left-hand menu, access the newly-created cluster, create a new domain and give it a name; for example, **Master**.

b. From the Site menu, add the line state servers (LSS) using the host names that the CTC servers used previously.

c. Create a CTC cluster, use the LSS create in the previous step. If two are configured, use one as the primary NeTS and one as the secondary.

Standard Parameter Fields, page 8-22 and Standard Layout, page 8-23 show the static configuration on the Configuration Manager and Directory Manager.

Adding a Netwise Cluster to BVSM

- Identifying the Clusters and Servers in BVSM, page 8-3
- Adding a Hardware Group and Console Service to BVSM, page 8-6
- Netwise Server Configuration Performed by BVSM, page 8-8
- Manual Configuration to Integrate the Netwise Servers, page 8-11

Identifying the Clusters and Servers in BVSM

Before configuring BVSM for integrating Netwise, you must first add a cluster, and then add each server to the cluster. You need to add a cluster even if the solution includes one Netwise server.

The name of the cluster must be the same used when creating the static configuration on the Telephony Configuration Application (TCA) on the Netwise server.

To add a Netwise cluster and servers, perform the following steps:

Procedure

Step 1 From the BVSM main menu, select Network > Console Servers.

The system displays the Manage Operator Console screen.

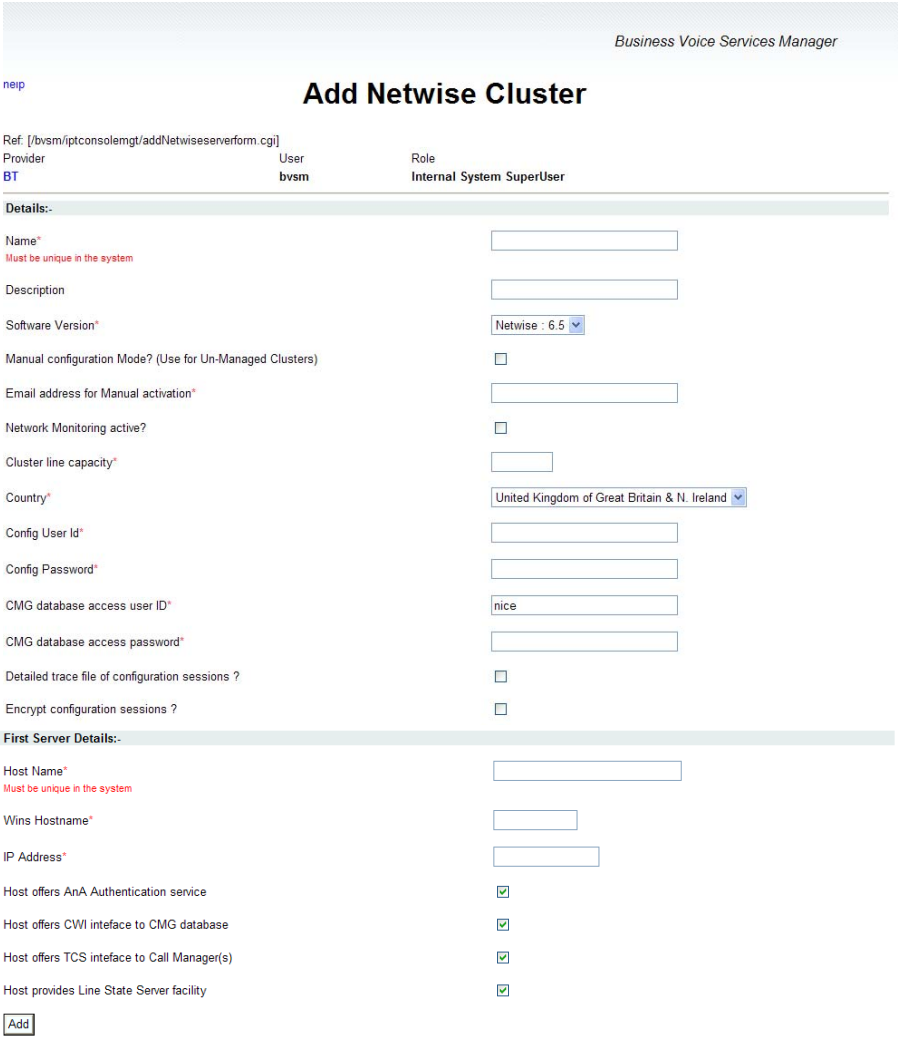
Step 2 On the Manage Operator Console screen, click **Add**.

The system displays the Product Selection screen.

Step 3 On the Product Selection screen, on the Netwise line, click **Add**.

The system displays the Add Netwise Cluster screen shown in Figure 8-1.

Figure 8-1 Add Netwise Cluster



Step 4 Type a name for the Netwise cluster that is unique in the BVSM system in the Name field.

The name of the cluster must be the same used when creating the static configuration on the Telephony Configuration Application (TCA) on the Netwise server.

Step 5 Choose the options that are appropriate for your Netwise implementation, such as the Netwise version number.

Step 6 In the First Server Details section, enter the host name and IP address of the first server in the Netwise cluster.

If the solution uses a single Netwise server, identify that server in the fields provided in this section.

Step 7 Enable the services that are appropriate for your Netwise server.

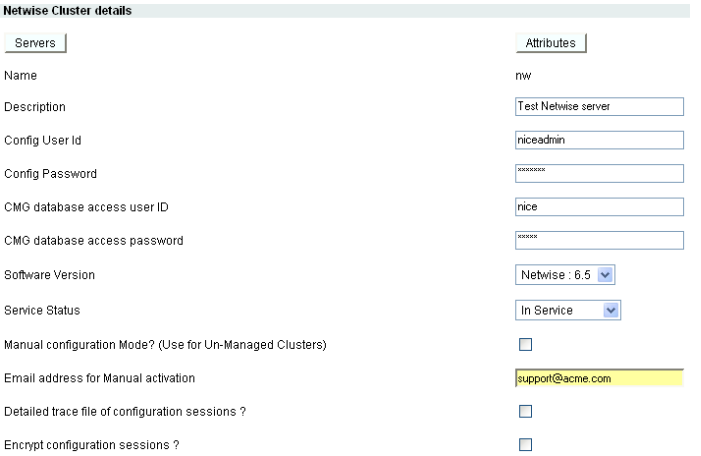
When adding the Netwise server, you must identify define the services that are associated with it; for example, AnA, CWI, TCS, TCA, and Line State.

Step 8 After completing the fields on the Details and First Server Details sections, click **Add** to add the cluster and the first server in the cluster.

Step 9 After adding the cluster, click the **Servers** button to add each additional server in the cluster.

The system displays Netwise Cluster Details screen, shown in Figure 8-2.

Figure 8-2 Netwise Cluster Details



Step 10 On the Netwise Cluster Details screen, click **Attributes**

The system displays the screen shown in Figure 8-3.

The default name for the configuration file is HUCS. Type the name of the configuration file for your Netwise server. You can use this screen to backup and restore your Netwise configuration file.

Figure 8-3 Netwise Configuration File

Adding a Hardware Group and Console Service to BVSM

Before adding the Netwise Operation Console Service, you must first create a hardware group that contains the Cisco PGW, Cisco Unified CM, and Netwise clusters to be configured.

To add the hardware group and console service, complete the following steps:

Procedure

Step 1 Choose **Networks > Hardware Groups > Add**.

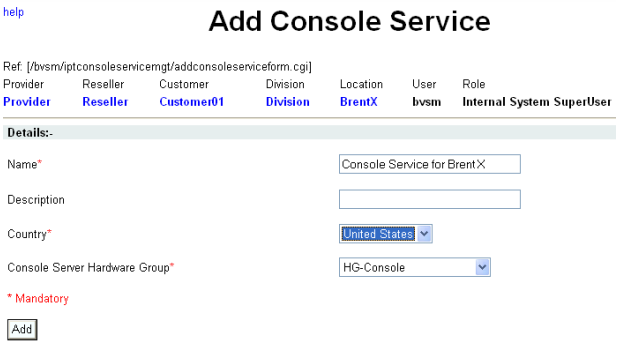
Step 2 Add the hardware group

For details about adding a hardware group, refer to Chapter 2, "Adding Cisco PGW-Cisco Unified CM Cluster Hardware Groups."

Step 3 To add a console service at the location level select **Resources > Console Service**.

The system displays the Add Console Service screen, shown in Figure 8-4.

Figure 8-4 Add Console Service



Step 4 Enter a name for the console service and select the hardware group that you defined in the previous step.

This ties the console service to a hardware group, which is a list of servers with defined functions. A hardware group supporting attendant console service would include Netwise, Unified CM, and Cisco PGW servers.

This transaction also defines a logical service in the BVSM database. This is a BVSM-only transaction and does not provision any other components such as Netwise and Unified CM.

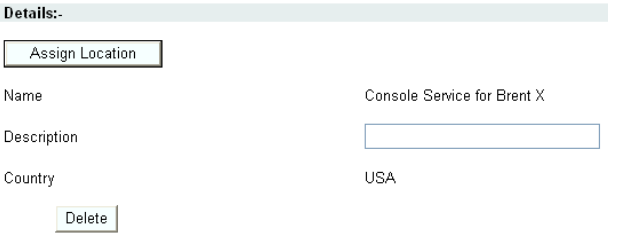
Step 5 Assign the console service to a location.

Locations within BVSM have a unique number ID or suffix assigned to them. This unique number ID or suffix is linked to every location. If required, customers can have overlapping naming conventions. The unique number ID or suffixes are used to configured network components. Within Netwise, they are used to provision sites, domains, customer group, customer view, and so on.

Note Only one operator console service can be added to a BVSM location.

The system displays the screen shown in Figure 8-5.

Figure 8-5 Assigning Console Service to a Location



Step 6 Click **Assign Location** and select the location from the screen that appears.

Netwise Server Configuration Performed by BVSM

After provisioning BVSM for the Netwise servers, BVSM automatically configures the Netwise servers, as described in the following topics:

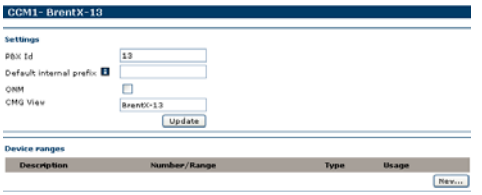
- CTC, page 8-8
- CMG, page 8-10

CTC

The following are provisioned in CTC:

- A domain—CTC assigns the correct customer view for that location (see Figure 8-6). The customer view is determined earlier with when provisioning CMG.

Figure 8-6 Domain Provisioning



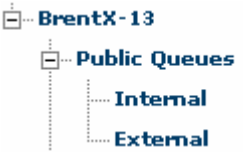
Note The Device Ranges section is not currently completed by BVSM. This includes the CTI Ports for Call Park, Camp On, Phones, and CTI Ports. These need to be defined manually after the BVSM provisioning.

- One site—Provisioned per BVSM location, it appears in the syntax shown in Figure 8-7.

Figure 8-7 Site Provisioning

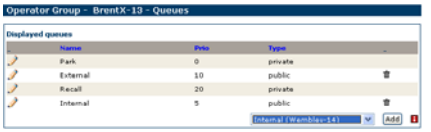
- A public queue—With internal, external, park (private) and recall (private) queues (see Figure 8-8). By default, public queues, park, and recall are private. This can be manually changed if required in operator groups through the TCA.

Figure 8-8 Public Queues Provisioning



- An operator group—This is associated with the public queues (see Figure 8-9). BVSM automatically assigns the default public queues to the operator group, internal, external, park, and recall queues.

Figure 8-9 Operator Group Provisioning



CMG

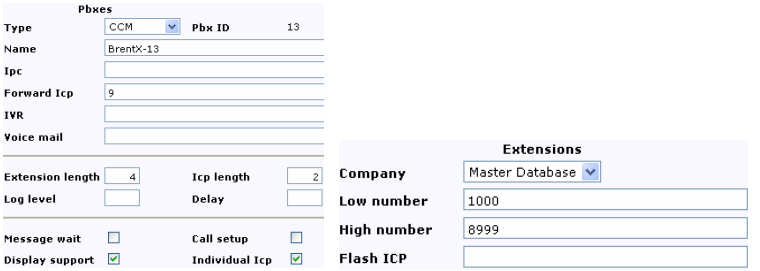
CMG provisions the following:

- A customer group—The name appears as the location name followed by the location suffix (see Figure 8-10). The Customer Group ID is also determined by the location suffix, as explained above.

Figure 8-10 Customer Group Provisioning

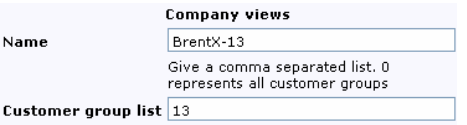
- PBX and extension range—The extension range defaults the complete range of 1000 to 8999 if a four-digit extension range was selected. The zero range is reserved for attendant console usage. Within this range are found the CTI Ports and Pilot numbers. The 9XXX range has been reserved for breakout and emergency dialing. (See Figure 8-11.)

Figure 8-11 PBX and Extension Range Provisioning



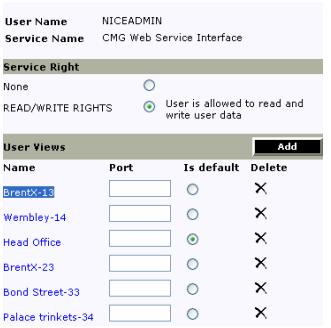
- Customer View—Controls the location to which the console service has been assigned (see Figure 8-12). By default, BVSM provisions only a customer view controlling the location to which it has been assigned. If required, extra customer group IDs can be added ad hoc through Netwise CM.

Figure 8-12 Customer View Provisioning



- Customer view to the administrative user, CMG web service interface—This is a default activity that should happen when a customer view is added (see Figure 8-13). This is a required transaction so that the Netwise administrative user can control amendments to the customer views.

Figure 8-13 Customer View Provisioning (Continued)



Manual Configuration to Integrate the Netwise Servers

This section describes the steps required on the CTC and Cisco Unified CM servers to complete the integration of the Netwise servers into the Hosted UCS implementation. This section includes the following topics:

- Configuring CTC, page 8-11
- Configuring Cisco Unified CM, page 8-13

Configuring CTC

Several manual steps are needed to complete in the CTC after BVSM completes the configuration transactions described in the "Netwise Server Configuration Performed by BVSM" section on page 8-8.

You must set up the device ranges for the route point, CTI park, CTI camp on, and phone range. Figure 8-14 shows an example. For the complete information, refer to the detailed design documentation.

Figure 8-14 Device Ranges

Device ranges

	Description	Number/Range	Type	Usage	
	RP23	(0201000020) 01XX	Route Point		
	CTI Port23	02010000200001 - 02010000200099	CTI port	Camp on resource	
	CTI Port23	02010000200001 - 02010000200099	CTI port	Park resource	
	Phone23	(0201000020) 1000 - 9999	Phone	Phone	

New...

In addition, you must add the new domains to the LSS servers and to the CTC servers serviced domains. (See Figure 8-15 and Figure 8-16.)

Figure 8-15 Adding the New Domains to LSS Servers

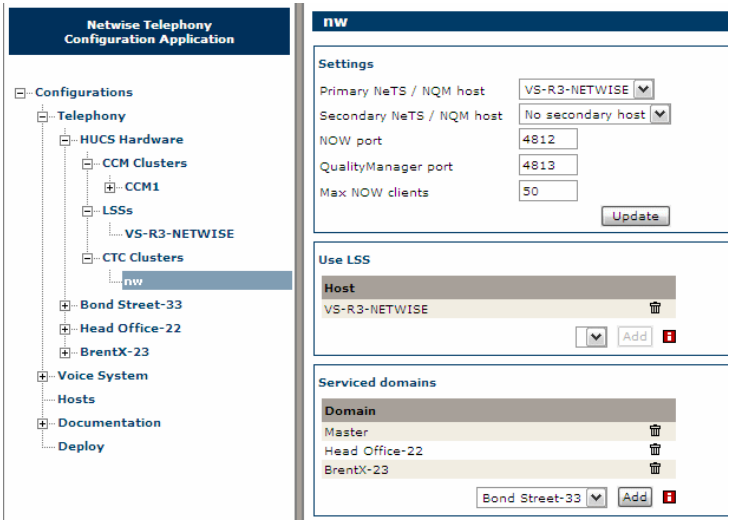
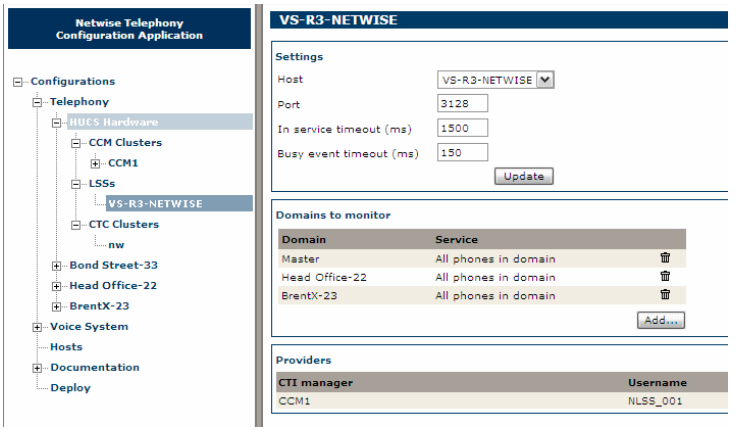


Figure 8-16 Adding the New Domains to CTC Servers



Configuring Cisco Unified CM

In the Cisco Unified CM, add the CTI route point for the location to be used by the queue pilot numbers. For complete information regarding naming and setup, refer to the detailed design documentation available from a VisionOSS technical consultant.

Configuring Operator Console Attributes

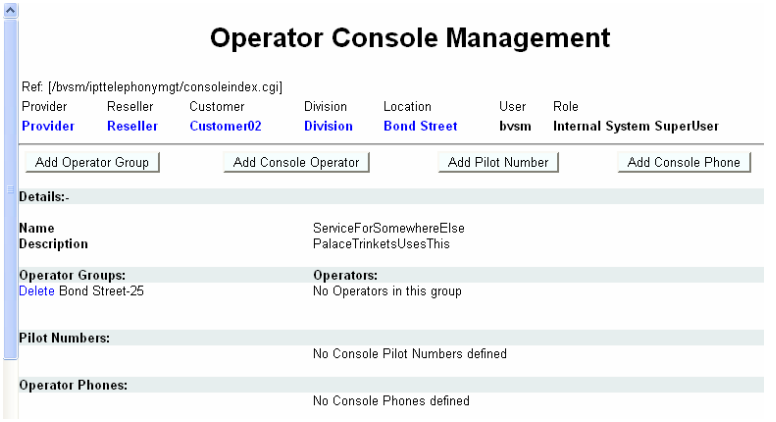
This section describes how to configure the operator console and includes the following topics:

- Configuring Operator Console Attributes, page 8-14
- Adding an Operator Group, page 8-14
- Adding a Console Operator, page 8-14
- CMG Configuration, page 8-15
- Manual Configuration to Add an Operator Console, page 8-15

Configuring Operator Console Attributes

From **Location Management > Telephony**, you can configure the console attributes (see Figure 8-17). These include configuring operator group, console operators, pilots numbers, and operator phones.

Figure 8-17 Configuring Console Attributes



Adding an Operator Group

This feature enables you to add extra operator groups. The operator group inherits the public queues of the location. BVSM automatically adds a default group <*location-name*>-<*location-suffix*> ready for use.

Adding a Console Operator

BVSM performs a lookup of all the users at that location. You can then assign a user as an operator.

CMG Configuration

This transaction enables a user to be able to use the console service. When you add a user, a transaction is applied that creates the user in CMG with the details shown in Figure 8-18. By default, the console operator is made an administrator of the Netwise directory and assigned the view for that location.

Figure 8-18 Adding a Console Operator

Note The user gets added to the CMG correctly; however, the password is not stored in CMG correctly. After the transaction completes, the password must be set in the CMG GUI so that it is stored correctly.

Manual Configuration to Add an Operator Console

This section describes steps required in the CTC and Cisco Unified CM server to complete the operator console configuration.

Cisco Unified CM

In the Cisco Unified CM, you must add a number of CTI ports for each operator that is assigned to the service. As a rule of thumb, ten CTI ports are recommended for each CTC server in the cluster. This generally means that 20 CTI ports are required to be added to the Cisco Unified CM. For complete information, refer to the detailed design documentation available from a VisionOSS technical consultant.

CTC

In the CTC server, you must add the console user to the operator group to which they are assigned. This is done in the CTC server under the operator group for the location in which you are working.

Adding a Pilot Number

This section describes the configuration for adding a pilot number and includes the following topics:

- Defining a Pilot Number, page 8-16
- Configuring CTC, page 8-17
- Configuring CMG, page 8-17

Defining a Pilot Number

When you define a pilot number, you must choose a public queue (see Figure 8-19). The default system public queues are internal and external. If the internal number has an E.164 number associated with it, this appears in the drop-down field. Associating E.164 number to internal numbers is done in the normal way and must be done before assigning it to a queue.

Figure 8-19 Adding a Pilot Number

When you have defined a pilot number, the number needs to be alpha tagged. This is required so that when the console operator monitors the queue, they can determine why people are dialing that queue. For example, if an internal pilot number of 0100 is mapped to the marketing department, this appears in the Console.

Several steps are required in the CTC and CMG servers after adding the pilot number to make the configuration work.

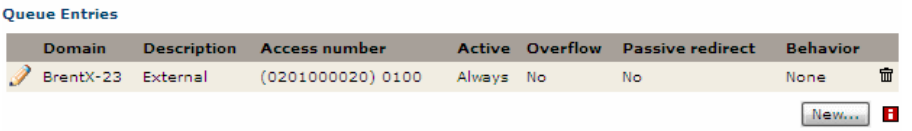
Configuring CTC

In the CTC, create the queue entry under the public queue required. The pilot number should match the number setup in BVSM. For complete information, refer to the detailed design documentation available from a VisionOSS technical consultant.

Configuring CMG

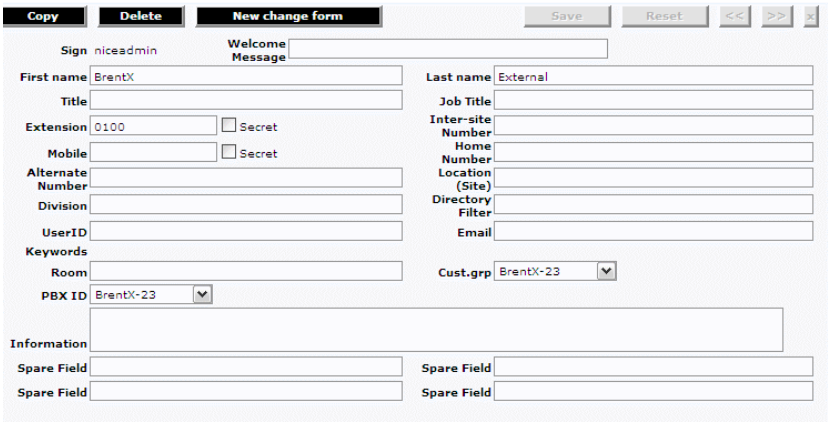
When a pilot number is added to a queue, BVSM needs to configure that number as a queue entry under the public queue in the CTC server. (See Figure 8-20.)

Figure 8-20 Configuring a Queue Entry



In the CMG Directory Manager, create a new user with the queue name, location name, and queue extension details (see Figure 8-21). For complete information, refer to the detailed design documentation available from a VisionOSS technical consultant..

Figure 8-21 Creating a New User



Adding a Console Phone

When you have defined the MAC address of the operator phone, it associates the primary extension of the phone so that it can be managed by TAPI. The phone should already have been registered with an appropriate FeatureGroup, assigning the correct attendant console class of service. This needs to be done manually in Cisco Unified CM. (See Figure 8-22.)

Figure 8-22 Adding a Console Phone

A manual step is required at this stage in the Cisco Unified CM servers to get the configuration working.

In the Cisco Unified CM, associate the phone with any NETS users setup in the Cisco Unified CM directory.

Managing Users

Users must be added to the Netwise directory so console operators can look up their details and verify their line states.

Note the following user directory rules:

- Extension mobility (roaming profile)—First line always takes precedence over the associated phone number extension and contact number. This means the primary extension number for extension mobility profile (roaming profile) is shown in the Netwise directory.
- If an extension mobility profile (roaming profile) is not defined and an associated phone is, and contact number details are filled out, the associated phone first extension takes precedence in the Netwise directory.
- If no extension mobility (roaming profile) or associated phone has been associated, the contact number is added in the Netwise directory. This can be used for local services such as taxi numbers, restaurants, and so on.

Using Netwise Tools

This section summarizes the tools available in Netwise for managing resources. It includes the following topics:

- Synchronizing Directories, page 8-20
- Synchronizing Netwise Assigned BVSM Locations, page 8-20
- Synchronizing Netwise Assigned Console Operators, page 8-21
- Releasing all Console Services from a Location, page 8-21
- Releasing all Console Operators for a Location, page 8-21
- Destroying a Location, page 8-22

Synchronizing Directories

BVSM lets you synchronize the users of a location with a newly-defined console service. This feature allows you to use a single transaction to synchronize the users of the customer with the Netwise directory. This can also be activated when the two systems have become out of sync, or when a console service is assigned to a location that already has users.

This is a one-way replication process, so if you manually add a user in directory manager, which is an unsupported activity, it is not replicated back into the BVSM user database. If a user is manually added and a synchronization occurs, BVSM does not delete the manually-configured user. This feature has been added to allow flexibility in the Netwise directory.

This feature is shown in the Network element, by selecting Console Cluster > Tools. (See Figure 8-23.)

Figure 8-23 Directory Synchronization

Synchronizing Netwise Assigned BVSM Locations

This tool is designed in case of a Netwise component failure. BVSM can redeploy an already-defined configuration to blank Netwise components. This tool re-deploys all BVSM console services for a given console server.

Note that if manual configuration is done on TCA, it is overwritten with BVSM sourced information.

Note This does not replace the need for backups.

Synchronizing Netwise Assigned Console Operators

To synchronize Netwise assigned console operations, select **Network > Console Operations**, select the console operator, and click **Tools**.

Note If manual configuration is performed on TCA, it is overwritten with BVSM sourced information.

This tool is designed in case of a Netwise component failure or a manual administration error on the Netwise server. BVSM can redeploy an already-defined configuration to blank Netwise components. This tool restores the console users of which BVSM is aware.

Note This does not replace the need for backups.

Releasing all Console Services from a Location

The Release all Console Services from Location tool removes console services from that location. The following transaction happens when this is activated:

- All Console Services at that location are queried
- A Release Console Service is issued for all console services found at that locations.

Releasing all Console Operators for a Location

The Release Console Operators for a Location tool does the following:

- Queries all operators at that location
- Un-assigns users with console rights

Destroying a Location

The Destroy tool has been improved to support console services. When a destroy is issued, it now includes the following transactions:

- Release all console operators for a location
- Release all console services from a location

Standard Parameter Fields and Standard Layout

This section includes the following topics:

- Standard Parameter Fields, page 8-22
- Standard Layout, page 8-23

Standard Parameter Fields

The field names in CMG should be set as shown in Table 8-1. They need to match what is configured in the Netwise driver. The driver is hard-coded to the parameters shown. These fields are managed by BVSM.

Any additional fields can be added; however, they need to be managed manually via the CMG configuration and not by BVSM. BVSM does not overwrite the information stored in the additional fields.

Table 8-1 Field Names

Field function	Field name	Labeled
First name	F_name	
Last name	L_name	
Extension	Telno	
Directory Filter	Dep1	
Location (Site)	Dep2	
Division (Tenant)	Div	
Inter-site Number	Misc1	

Table 8-1 Field Names

Mobile Number	Cordless	
Home Number	Misc3	
Alternate Number	Misc4	
UserID	Misc5	
Email	Misc6	
Title	Misc7	
Job Title	Misc8	
Room	Misc9	
Information	Misc10	
Spare (Optional)	Misc11	
Spare (Optional)	Misc12	
Spare (Optional)	Misc13	
Spare (Optional)	Misc14	
Welcome Message	Misc15	

Standard Layout

Figure 8-24, Figure 8-25, and Figure 8-26 show the recommended presentation for the operator console. This can be changed but must include the default parameters as shown above. To edit this layout, go to Netwise Directory Manager > Standard Layouts and change the views for the main form, record list, and search record.

Figure 8-24 Operator Console (1)

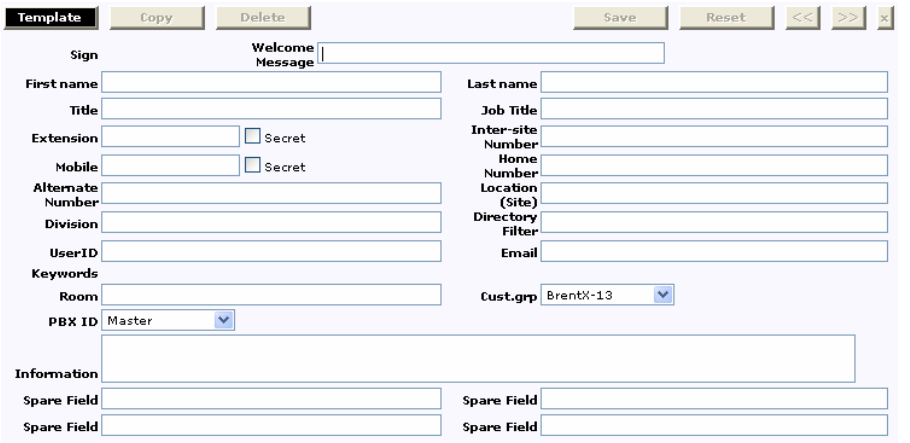
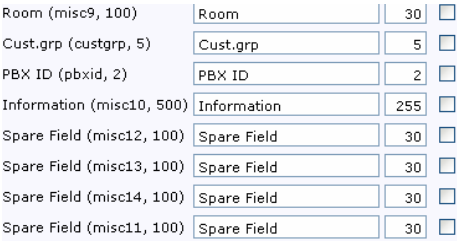


Figure 8-25 Operator Console (2)

Default (dbname, max)	Name default	Size	RO
Sign (sign, 16)	Sign	8	☑
Welcome Message (misc15, 100)	Welcome Message	50	☐
First name (fname, 60)	First name	30	☐
Last name (lname, 60)	Last name	30	☐
Title (misc7, 100)	Title	30	☐
Job Title (misc8, 100)	Job Title	30	☐
Extension (telno, 60)	Extension	30	☐
Inter-site Number (misc1, 100)	Inter-site Number	30	☐
Mobile (cordless, 60)	Mobile	30	☐
Home Number (misc3, 100)	Home Number	30	☐
Alternate Number (misc4, 100)	Alternate Number	30	☐
Division (div, 30)	Division	30	☐
Location (Site) (dep1, 30)	Location (Site)	30	☐
UserID (misc5, 100)	UserID	30	☐
Email (misc6, 100)	Email	30	☐
Keywords (subject, 30)	Keywords	200	☐

Figure 8-26 Operator Console (3)



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 VisionOSS BVSM 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, page 9-1
- Provisioning Unified CM to Support NAT/PAT, page 9-4
- Provisioning BVSM to Support NAT/PAT, page 9-9

Support for NAT/PAT

This section describes support for NAT/PAT through autoregistration of IP phones when VisionOSS BVSM 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, page 9-2
- Supported Scenarios for DHCP Services, page 9-2
- How IP Phone Autoregistration Provides NAT/PAT Support, page 9-3
- Limitations in Support for NAT/PAT, page 9-4

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 VisionOSS BVSM. BVSM depended on IP address information from the DHCP server to determine the location of phones, and this was a dependency for the BVSM AutoMove feature.

When BVSM 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 BVSM 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 BVSM 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 BVSM 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 BVSM. This allows the DHCP server to be separated from the BVSM 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 BVSM AutoMove feature is received through the syslog messages provided by the Unified CM Server.

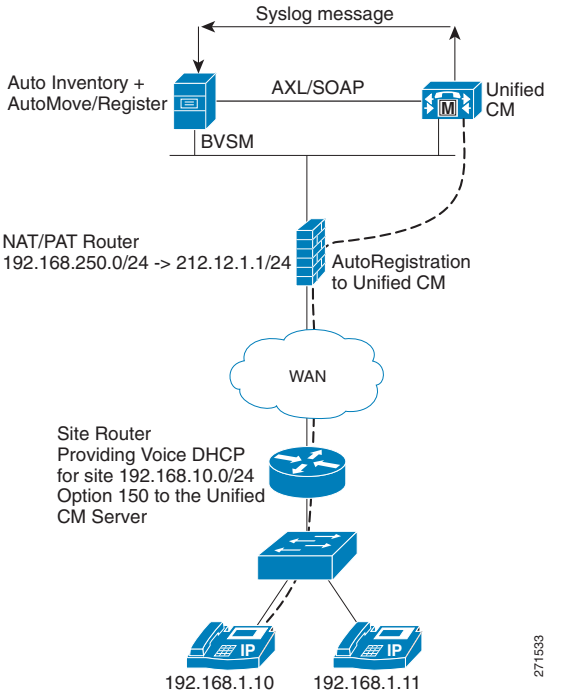
Supported Scenarios for DHCP Services

BVSM now supports DHCP services in the following scenarios, using auto-registration provided by the Unified CM server:

- DHCP services managed by BVSM, running on the BVSM server
- DHCP services managed by BVSM, running on an external server
- DHCP services *unmanaged* by BVSM, running on an external server
- DHCP services unmanaged by BVSM, 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 9-4.

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 BVSM server receives a syslog message from Unified CM, the AutoReg service picks it up from the log and triggers the AutoCCMNewPhone transaction in BVSM. 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 BVSM 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 BVSM, the transaction updates the BVSM 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 BVSM with an allocated extension number.

BVSM 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 BVSM, the DHCP server and the BVSM 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 BVSM manages the DHCP server, customer locations in different subnets connected to a common PAT router are not supported because BVSM 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 BVSM 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 BVSM server through a Cisco NAT/PAT device. It includes the following topics:

- Auto-registration, page 9-5
- Configuring Auto-registration, page 9-5

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 BVSM 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:

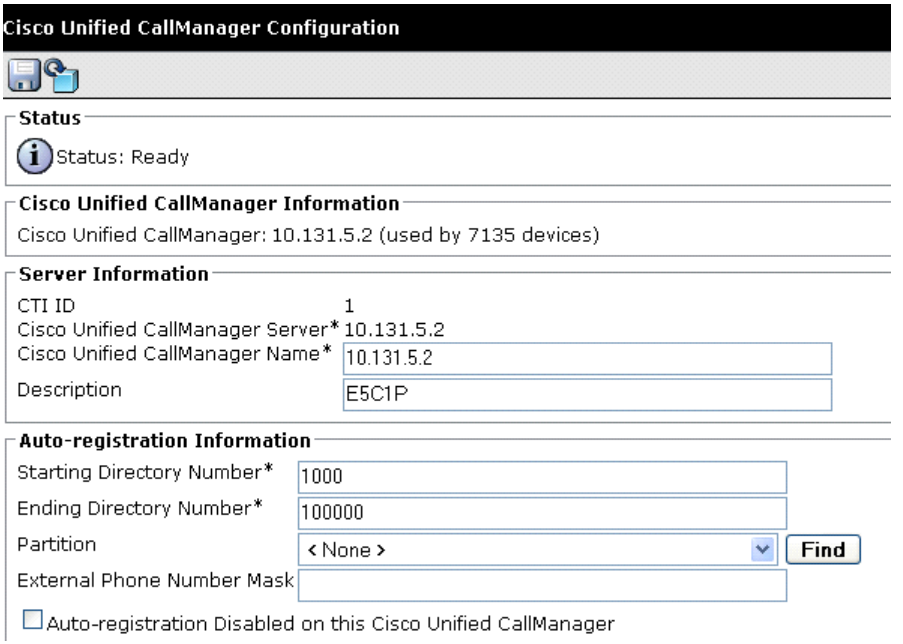
Procedure

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



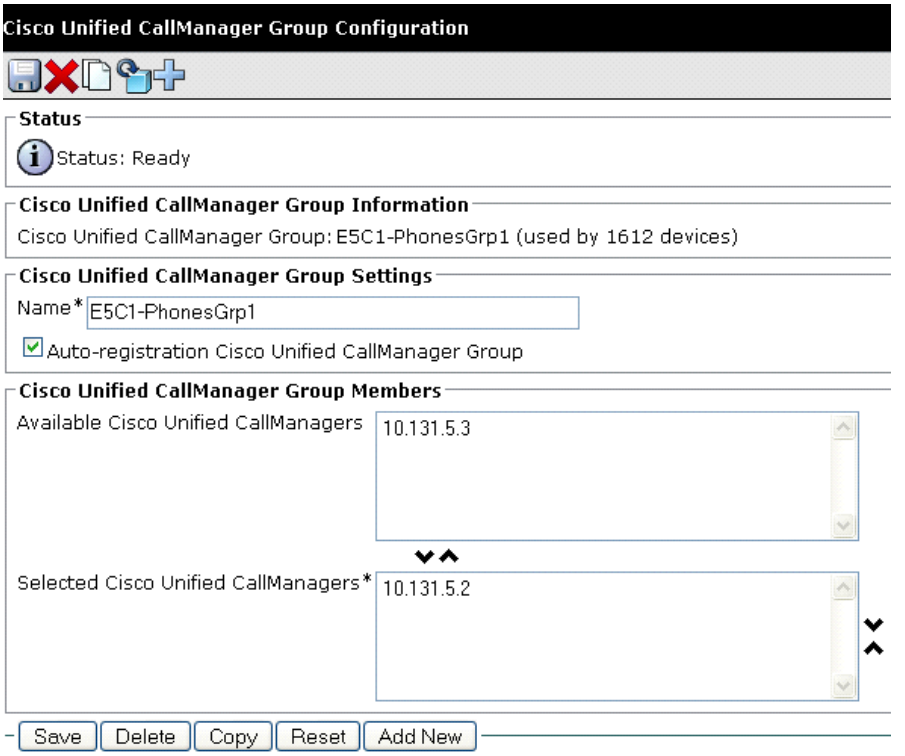
Step 4 Make sure that **Auto-registration Disabled on this Cisco Unified CallManager** is unchecked.

Perform this step for all the Unified CM servers.

Step 5 Choose **System > Cisco Unified Call Manager Group**.

The system displays the screen shown in Figure 9-3.

Figure 9-3 Auto-registration – Unified CM Group Configuration

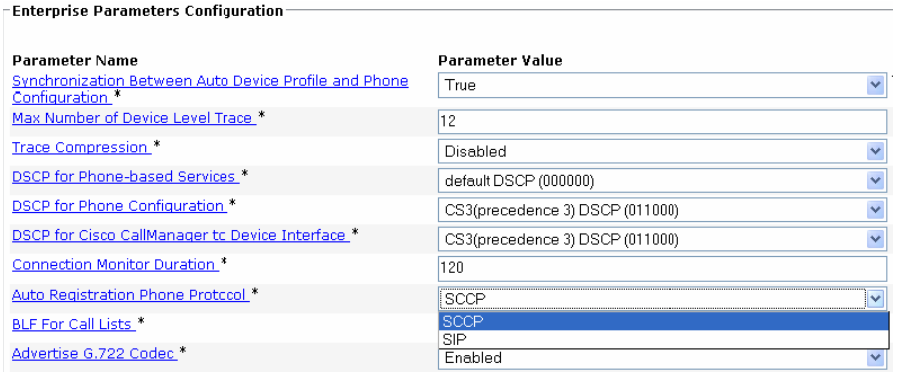


Step 6 Enter the group used in the Name field and check **Auto-registration Cisco Unified CallManager Group**.

Step 7 Choose **System > Enterprise Parameters Configuration** screen.

The system displays the screen shown in Figure 9-4.

Figure 9-4 Auto-registration – Call Control Protocol



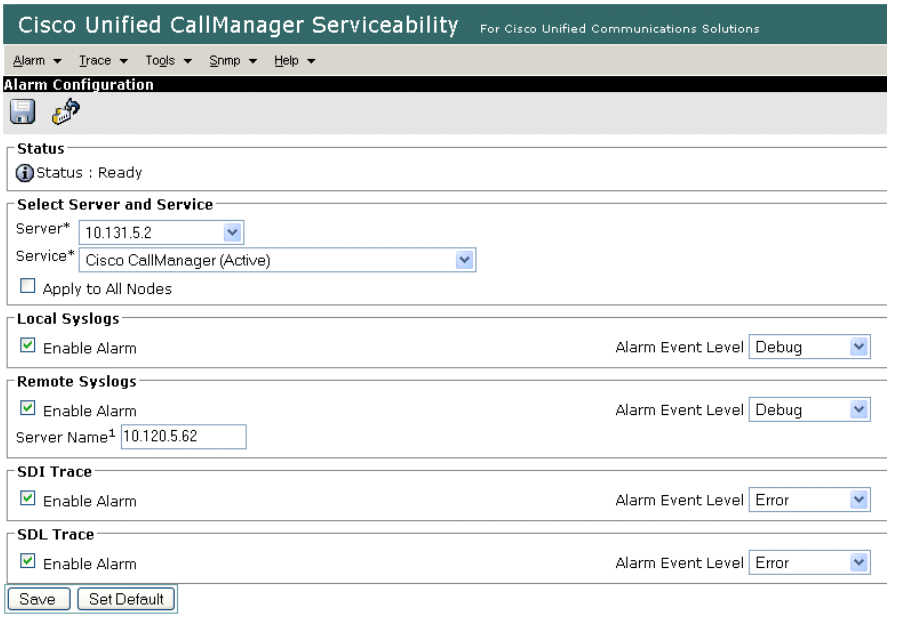
Choose the correct protocol (SIP or SCCP) from the **Auto-registration Phone Control Protocol** pull-down selection list.

Perform this step for Unified CM 5.1 and above. Unified CM 4.X supports only the SCCP protocol.

Step 8 To direct Unified CM Syslog Messages to the BVSM Server, select **Cisco Unified CallManager > Alarm Configuration**.

The system displays the screen shown in Figure 9-5.

Figure 9-5 Syslog Configuration on Unified CM



Step 9 In the Remote Syslogs section, type the IP address of the BVSM server in the Server Name field.

Step 10 Click **Save**.

Provisioning BVSM to Support NAT/PAT

This section describes the configuration required for the BVSM server when it is connected to IP phones by a Cisco NAT/PAT device. It includes the following topics:

- Configuring BVSM Webmin, page 9-10
- BVSM Provider Configuration, page 9-16
- BVSM Customer Configuration, page 9-18
- BVSM Location Administration, page 9-21

Configuring BVSM Webmin

To complete the configuration required using BVSM Webmin, complete the following steps:

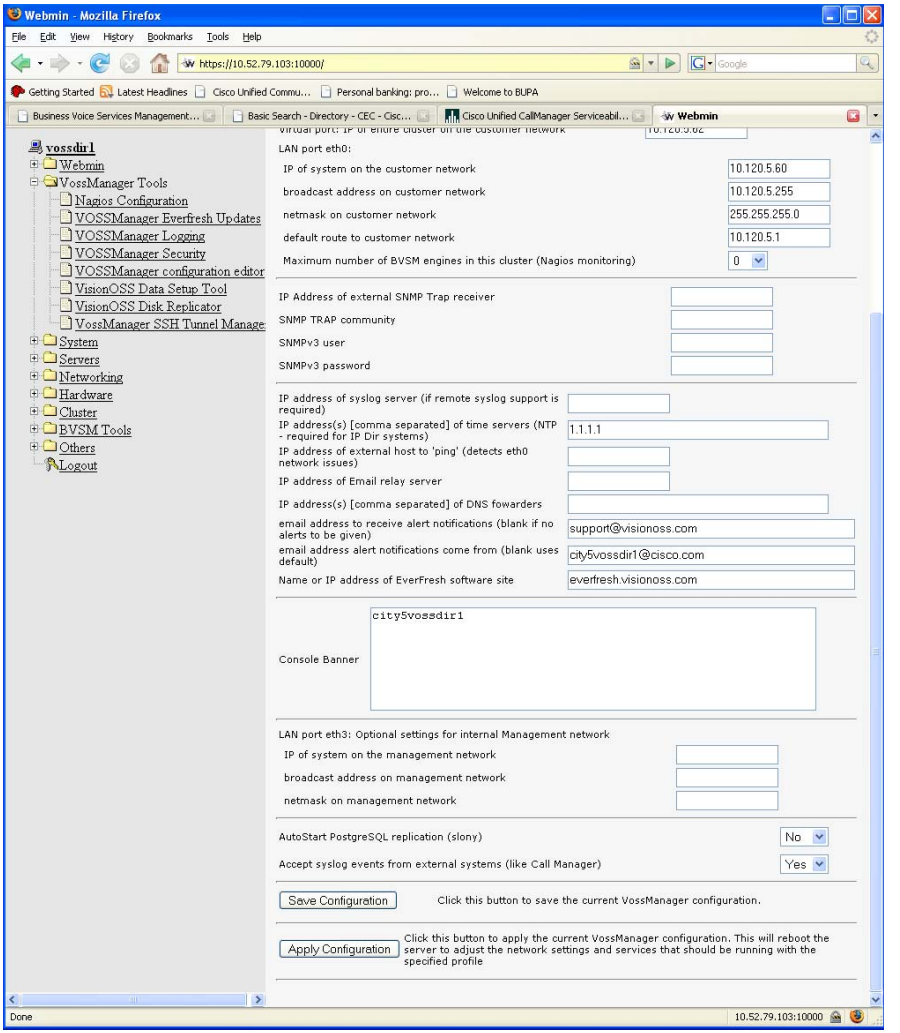
Procedure

Step 1 Access BVSM Webmin.

Step 2 Choose **VossManager Tools > VossManager configuration editor.**

The system displays the screen shown in Figure 9-6.

Figure 9-6 BVSM Webmin Syslog Configuration

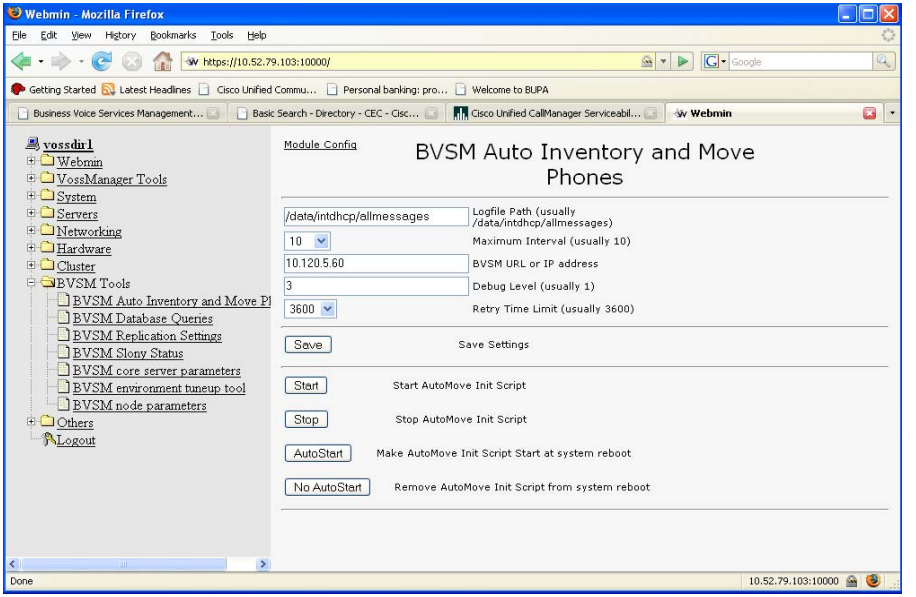


Step 3 Choose **Yes** from the **Accept syslog events from external systems (like call Manager)** pull-down selection list.

Step 4 Choose **BVSM Tools > BVSM Auto Inventory and Move Phones**.

The system displays the screen shown in Figure 9-7.

Figure 9-7 BVSM Auto Inventory/Move Phone Log Path



Step 5 In the Logfile Path field, type the following path:

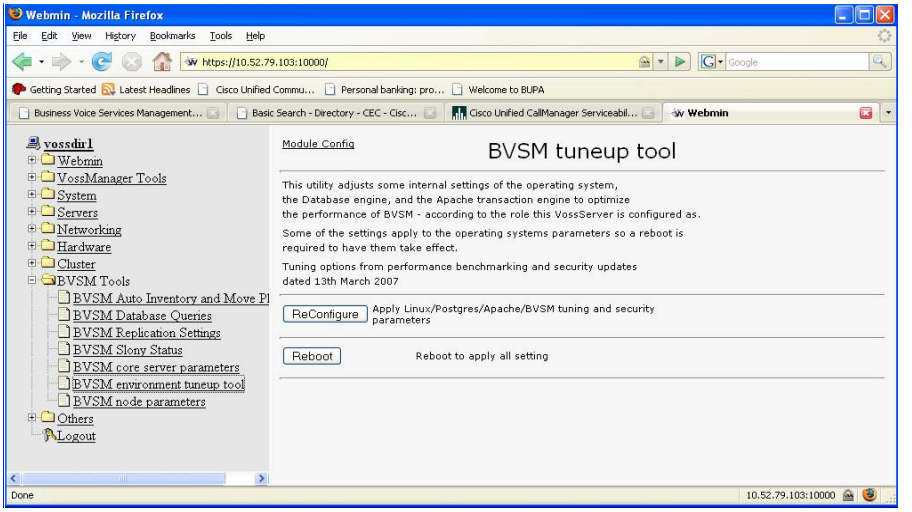
```
/data/intdhcp/allmessages
```

Step 6 Click **Start** and **Auto-start**.

Step 7 To reboot the BVSM server, select **BVSM Tools > BVSM environment tuneup tool**.

The system displays the screen shown in Figure 9-8.

Figure 9-8 BVSM Tune-Up Tool



After making changes to the BVSM server configuration, you must reboot the server to enable the changes.

Step 8 Click **Reboot**.

The BVSM server reboots and the new configuration is enabled.

Step 9 To verify correct syslog configuration for the BVSM server, establish an SSH session to the BVSM server using the administrator username/password.

Step 10 To display the messages received by the BVSM 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 BVSM server.

Configuring DHCP Services on an External Server

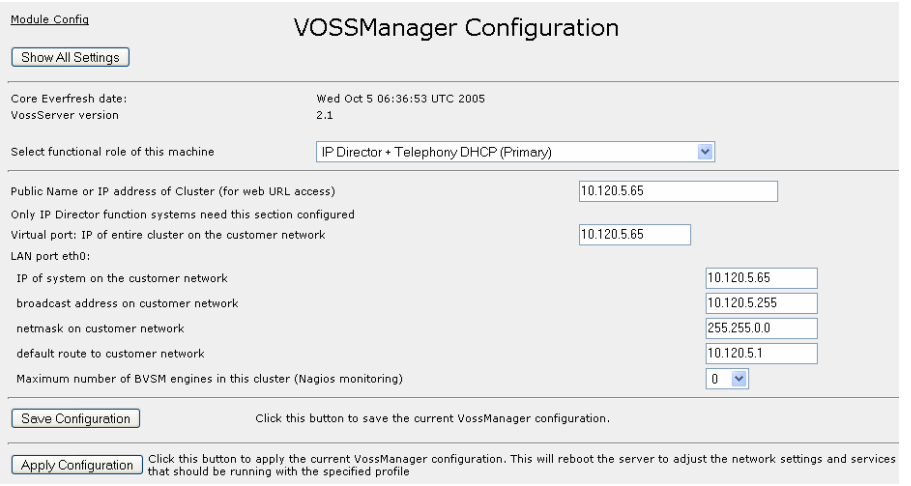
To configure DHCP services running on an external server, complete the following steps on the webmin of the external DHCP server:

Procedure

Step 1 Choose **Voss ManagerTools > VossManager Configuration**.

The system displays the screen shown in Figure 9-8.

Figure 9-9 BVSM External DHCP Webmin Configuration



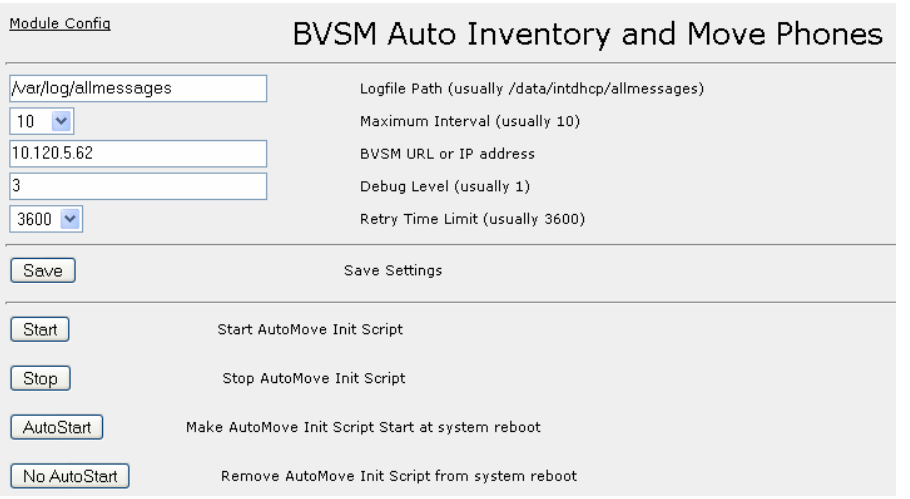
Step 2 Select **IP Director + Telephony DHCP (Primary)** from the **Select functional role of this machine** pull-down selection list.

Step 3 Click **Save Configuration** and **Apply Configuration** to save and apply the configuration.

Step 4 Choose **BVSM Tools > BVSM Auto Inventory and Move Phones.**

The system displays the screen shown in Figure 9-9.

Figure 9-10 BVSM External DHCP Webmin BVSM Tools configuration



Step 5 In the BVSM URL or IP address, type the IP address or URL for the BVSM server.

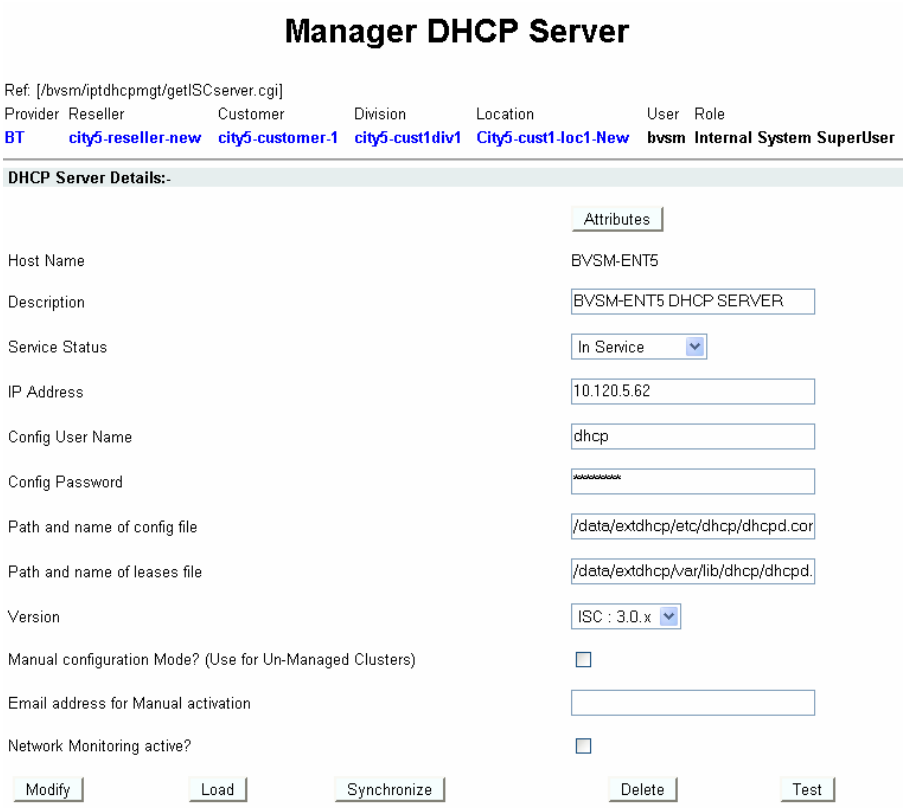
Step 6 Click **Save** and **Start** to save the settings and start the AutoMove feature.

BVSM DHCP Configuration

The configuration for a DHCP server managed by BVSM is similar whether it runs on the BVSM server or on an external server. However, you use the IP address of the BVSM server if the DHCP service is running on the BVSM server machine. You use the IP address of the external server if the DHCP service is running on a different machine.

Figure 9-11 illustrates the screen used in the BVSM GUI to configure the DHCP service.

Figure 9-11 BVSM DHCP Configuration



Make sure, once the DHCP server is defined on BVSM, the server is Loaded and Synchronized.

BVSM Provider Configuration

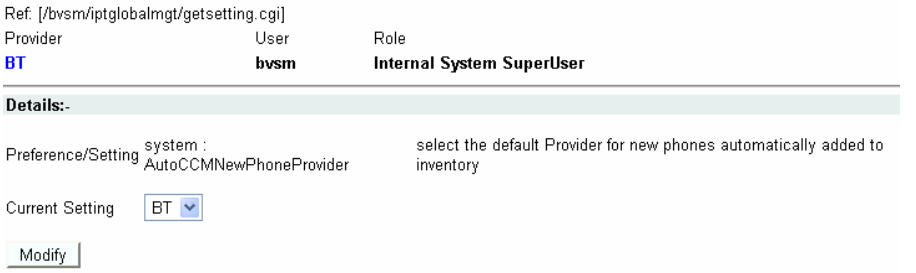
To configure the BVSM server to receive Auto-register requests from the Unified CM server, complete the following steps:

Procedure

Step 1 Choose **Setup Tools > Global Settings > AutoCCMNewPhoneProvider**.

The system displays the screen shown in Figure 9-12.

Figure 9-12 BVSM Register Setting

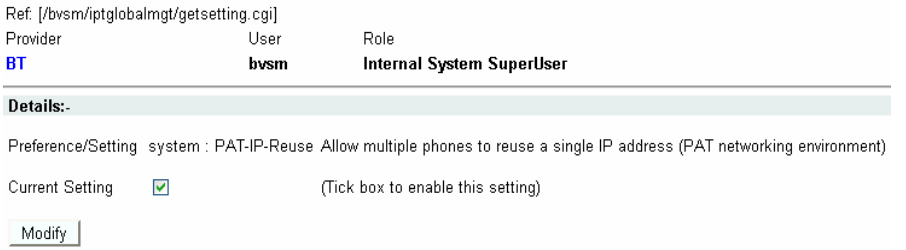


Step 2 Choose the provider to which the Auto-register daemon reports.

Step 3 Choose **Setup Tools > Global Settings > PAT-IP-Reuse.**

The system displays the screen shown in Figure 9-13.

Figure 9-13 BVSM PAT Setting



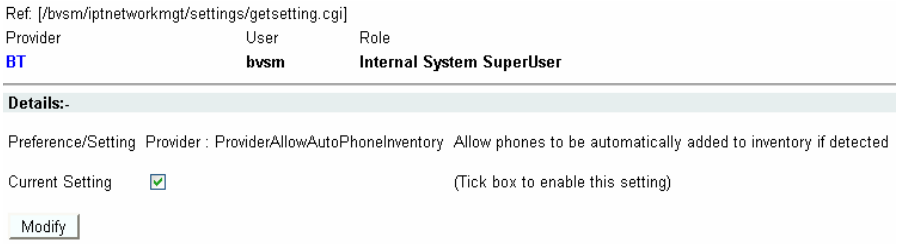
Step 4 Enable the **Current Setting** checkbox.

This setting is used when phones register with the same IP address (PAT).

Step 5 Choose **Provider > Select a provider > Preferences > ProviderAllowAutoPhoneInventory.**

The system displays the screen shown in Figure 9-14.

Figure 9-14 BVSM Provider Allow Auto Inventory Phone Setting



Step 6 Enable the **Current Setting** checkbox.

This causes BVSM to automatically add phones discovered through Auto-registration to the Phone Inventory.

BVSM Customer Configuration

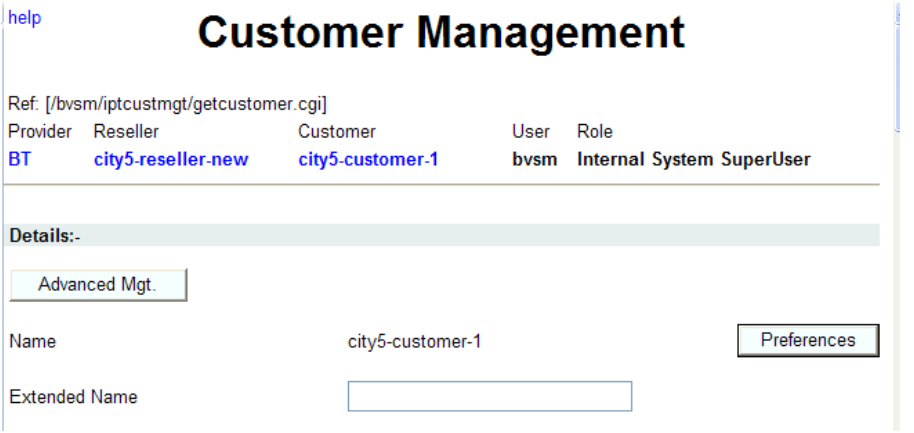
To complete the Customer configuration required on the BVSM server, complete the following steps:

Procedure

Step 1 Choose the customer for which you want to enable the AutoMoveCustomer option.

The system displays the screen shown in Figure 9-15.

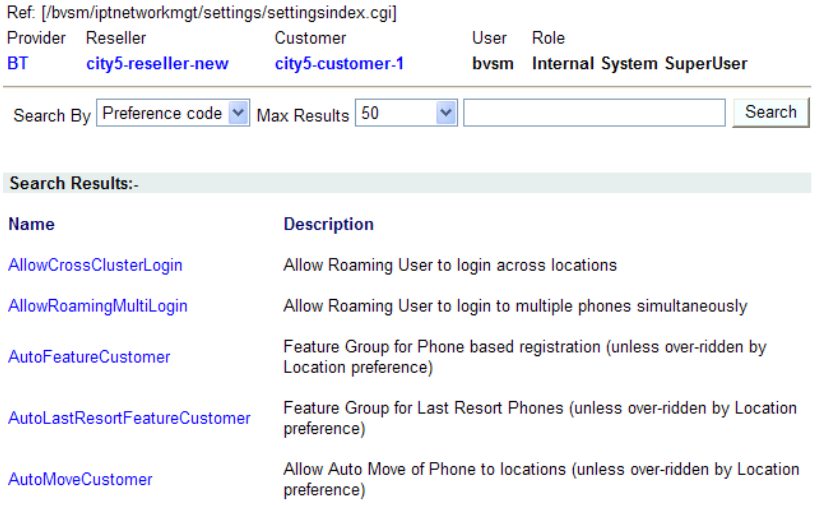
Figure 9-15 Customer Management



Step 2 Click **Preferences.**

The system displays the screen shown in Figure 9-16.

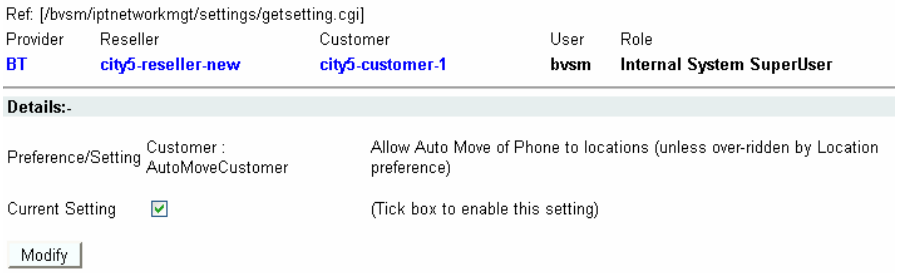
Figure 9-16 Preferences and Settings



Step 3 Click **AutoMoveCustomer**.

The system displays the screen shown in Figure 9-17.

Figure 9-17 BVSM CustomerAutoMove Setting

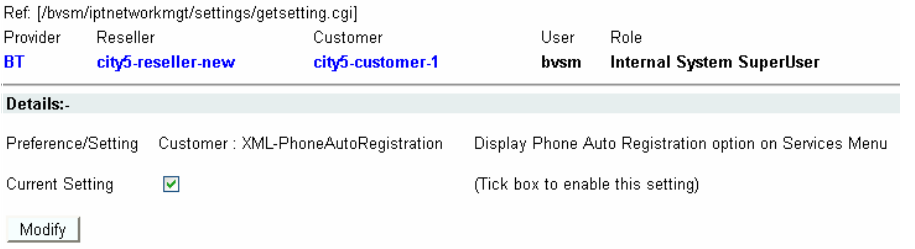


Step 4 Enable the **Current Setting** checkbox.

Step 5 On the Preferences and Settings screen (Figure 9-16), click **XML-PhoneAutoRegistration**.

The system displays the screen shown in Figure 9-18.

Figure 9-18 BVSM XML-PhoneAuto-Registration Setting

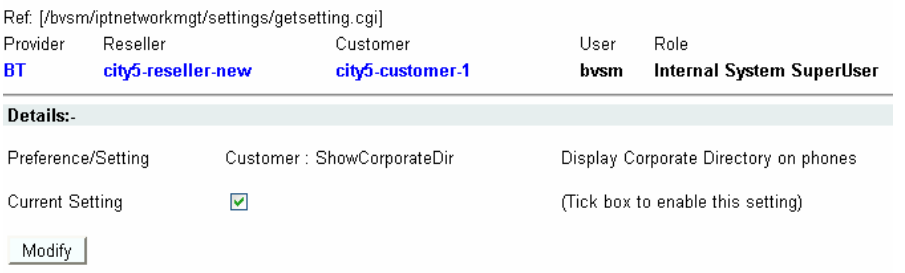


Step 6 Enable the **Current Setting** checkbox.

Step 7 On the Preferences and Settings screen (Figure 9-16), click **ShowCorporateDir**.

The system displays the screen shown in Figure 9-19.

Figure 9-19 BVSM Directory Services Setting



Step 8 Enable the **Current Setting** checkbox.

BVSM Location Administration

Step 1 Choose the Location for which you need to enable the AutoMove feature.

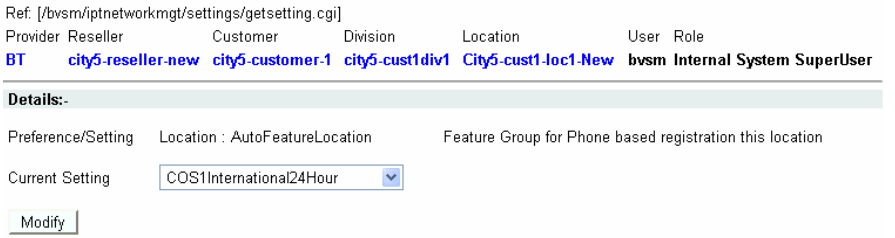
The system displays the screen shown in Figure 9-20.

Figure 9-20 BVSM Directory Services Setting

Step 2 Click **Preferences** and select the **AutoFeatureLocation** option from the Preferences and Settings: Location screen.

The system displays the screen shown in Figure 9-21.

Figure 9-21 BVSM Location Feature Group Setting

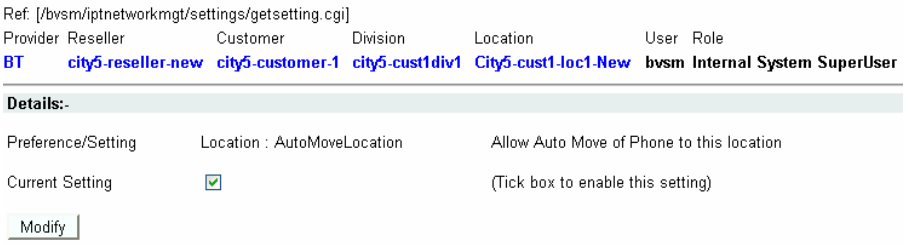


Step 3 Choose the appropriate feature group, such as **COS1International24Hour**.

Step 4 From the Preferences and Settings: Location screen, select the **AutoMoveLocation** option.

The system displays the screen shown in Figure 9-22.

Figure 9-22 BVSM AutoMove Location Setting

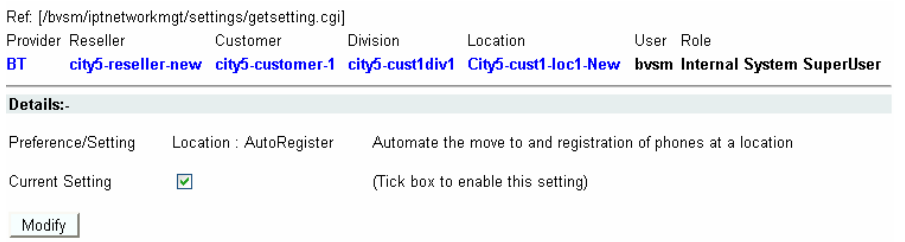


Step 5 Enable the **Current Setting** checkbox.

Step 6 From the Preferences and Settings: Location screen, select the **AutoRegister** option.

The system displays the screen shown in Figure 9-23.

Figure 9-23 BVSM AutoRegister Location Setting

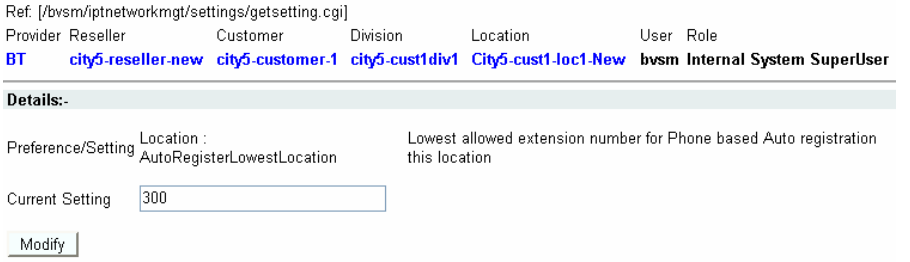


Step 7 Enable the **Current Setting** checkbox.

Step 8 From the Preferences and Settings: Location screen, select the **AutoRegisterLowestLocation** option.

The system displays the screen shown in Figure 9-24.

Figure 9-24 BVSM AutoRegister DN Location Setting



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 BVSM server to enable the new configuration.

CHAPTER 10

Provisioning Shared Building

This chapter describes the steps required to configure the Shared Building feature introduced with Cisco Hosted Unified Communications Services, Release 6.1(a).

The chapter details how to use VisionOSS BVSM application to manage resources and provision network elements of a MultiTenant Hosted UCS 6.1(a) deployment.

This chapter includes the following sections:

Building Administration

Building Adminitration involves the following tasks:

- Adding a Building, page 10-2
- Add Site Codes, page 10-5
- Add Building Voicemail Service, page 10-6
- Selecting VoiceMail Service Profile, page 10-7
- Add AutoAttendant Service, page 10-7
- Adding and Moving E164 Numbers to VoiceMail Service for the VoiceMail and AutoAttendant Service Pilot Numbers, page 10-8
- Add Feature Groups, page 10-9
- Adding Customer, Division, and Shared Building Location Including VoiceMail and AutoAttendant Services, page 10-10

Adding a Building

This feature allows you define Here you can define a number of Buildings. To create a Building, use the following steps:

Procedure

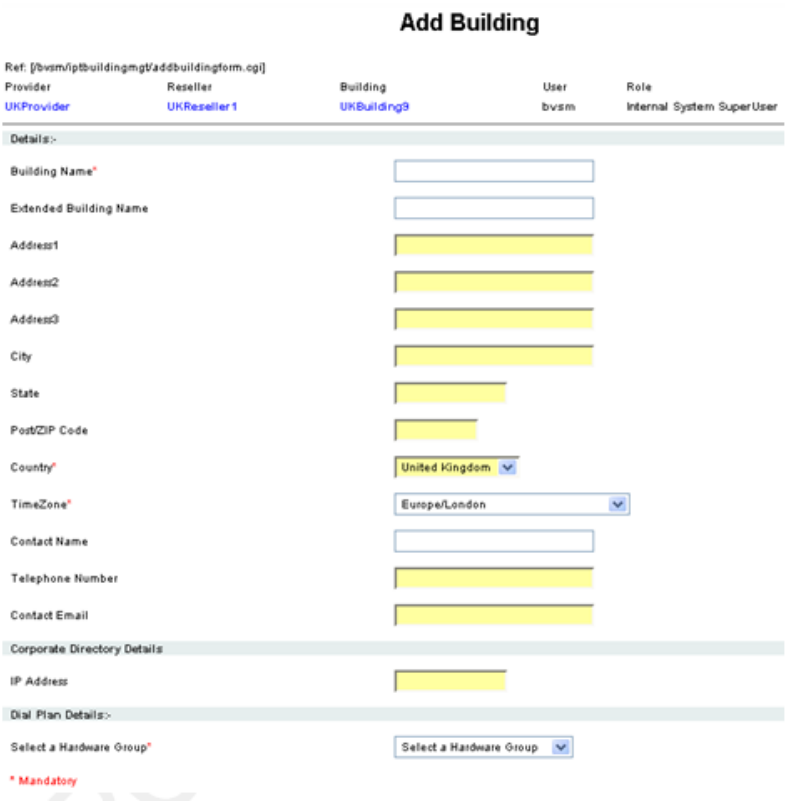
Step 1 Choose **General Administration > Building**.

The Building Management page displays.

Step 2 Click **Add**.

The Add Building page displays.

Figure 10-1 Adding a Building



Step 3 Under Details, add the following:

- Name: <ResellerName>; for example, UKBuilding1
- Extended Building Name: <ExtendedBuildingName>
- Address1: <AddressLine1>
- Address2: <AddressLine2>
- Address3: <AddressLine3>
- City: <City>
- State: <State>
- Post/Zip Code: <Post/Zip Code>

- Country: <Country>; for example, UK
- TimeZone: <TimeZone>
- Contact Name: <ContactName>
- Telephone Number: <ContactTelephoneNumber>
- Contact Email: <Contact

Step 4 <Under Corporate Directory Details, enter the following:

- IP Address: <IPAddress>

Step 5 Under Dial Plan Details, enter the following:

- Select a Hardware Group: Select a hardware group from the drop-down list box.

Step 6 Click **>>Next**, and enter the following dial plan details:

- IPPBX: Select the IPPBX from the drop-down list box.
- IP Edge Device: Select the IP Edge Device from the drop-down list box.
- Media Service Name: Select the Media Service Name from the drop-down list box.
- Inter-Site Prefix: Select the Inter-Site Prefix from the drop-down list box.
- External Access Prefix: Select the External Access Prefix from the drop-down list box.
- Building Area Code: Select the Building Area Code from the drop-down list box.
- PBX Template: Select the PBX Template from the drop-down list box.
- Voice Bandwidth (Kbps): <VoiceBandwidth>
- Video WAN Bandwidth (Kbps): <VideoWANBandwidth>

Note Additional device pools can also be created, if required, at the building level after the building has been created. To add additional device pools, in the Building Administration menu, click **Advanced Management > CCM Devicepool Management > Add**.

Note The Device Pool is not added to the CUCM at this stage. It only adds an entry to BVSM. While adding a location, you can select the Device Pool from a drop down menu which gets added to CUCM at the time.

This procedure updates BVSM and PGW.

Tip In order to avoid making additions to customers, division, and locations inside a Building at a later stage, configure Voicemail, AutoAttendant and Preference settings if any before creating the Customer, Divisions and Locations. This step is not mandatory. If at all a change needs to be made after creation of the customer, division and locations they can be modified at any stage.

Add Site Codes

Use the following steps to add site codes.

Procedure

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

Step 2 Click on the buildning name that you want to confgure site code for. The Building Management page displays.

Step 3 Click the **Site Codes** tab.

Step 4 Click **Add**.

Step 5 Under Details, add the following:

- Site Code: <number based on site code rule length>, 400. This is the starting range.
- Last Site Code in range: <number based on site code rule length>; for example, 405

Note Make sure that you complete VoiceMail/AutoAttendant related static configuration before proceeding to the next section.

Add Building Voicemail Service

Use the following steps to add a building VoiceMail.

Procedure

Step 1 In the Building Management page, click the VoiceMail tab. The Manage Building VoiceMail Service page displays.

Step 2 Click **Add**.

Step 3 Under Details, add the following:

- Name: <ResellerName>, for example: UKBuilding1VM1
- Country: <Country>, for example: UK
- Site code: <Code>, for example: 400
- Voice Mail Server Hardware Group: <Hardware Group>
- Extension Length: <Length>, example 4
- Voicemail PSTN Dial Prefix: <Prefix>, example 9

Step 4 Click **Next>>**.

Step 5 Under Details, add the following:

- Voicemail Server: Select a VoiceMail server from drop-down list box.

Note The Building VoiceMail service creates a VoiceMail dial plan on the PGW. This service is used by all customers in this building. Even though it possible to create an individual VoiceMail service for every customer in the building, this method is not recommended, as this is not very scalable on the PGW. For example, if there were 4000 customers in a building, then 4000 voicemail dial plans will be created on the PGW.

Selecting VoiceMail Service Profile

Use the following steps to select a VoiceMail service profile.

Procedure

Step 1 In the Building Management page, click the VoiceMail tab. The Manage Building VoiceMail Service page displays.

Step 2 Click the VoiceMail Profile Mgt tab. The Building VoiceMail Profile Management page displays.

Step 3 Under Available VoiceMail Service Profiles, Select the appropriate profile by selecting the appropriate checkboxes.

Add AutoAttendant Service

Use the following procedure to add the AutoAttendant service.

Procedure

Step 1 In the Building Management page, click the AutoAttendant tab. The Manage Building AutoAttendant Service page displays.

Step 2 Click **Add**. The Add Building AutoAttendant Service page displays.

Step 3 Under Details, add the following:

- Name: <ResellerName>, for example: UKBuilding1VM1
- Country: <Country>, for example: UK
- Voice Mail Server Hardware Group: <Hardware Group>
- Extension Length: <Length>, example 4
- Voicemail PSTN Dial Prefix: <Prefix>, example 9

Step 4 Click **Next>>**.

Step 5 Under Details, add the following:

Step 6 IVR Server: Select the IVR server from the drop-down list box.

Adding and Moving E164 Numbers to VoiceMail Service for the VoiceMail and AutoAttendant Service Pilot Numbers

Use the following steps to Add and Move E164 Numbers to VoiceMail service for the VoiceMail and AutoAttendant service pilot numbers.

Procedure

Step 1 Choose Resources > E164 Inventory.

Step 2 Select Country and click **Next>>**.

Step 3 Click **Area Code Mgt**.

Step 4 Under Defined Area Codes for Country, add the following:

Step 5 Select National Area code; for example, 1640

Step 6 Click **Next >>**.

Step 7 Click **Add Number Range**.

Step 8 Under Details, add the following:

- GBR : United Kingdom: <area code>; for example, 1640 (This is normally pre-populated)
- Start of number range: <range>; for example, 400100
- End of number range: <range>; for example, 400109

Note The example above creates 10 e164 numbers starting from 1640400100 to 1640400109.

Step 9 Return to the E164 Telephone Numbers menu.

Step 10 Click the **Move Number Range** tab.

Step 11 Under Details, add the following:

- Select Location: <VM service>, for example: UKBuilding1VM1 (Choose the Voicemail service created before)
- Start of number range: <range>, for example: 1640400100
- End of number range: <range>, for example: 1640400109

Add Feature Groups

Use the following steps to add a feature group:

Procedure

Step 1 Choose **General Administration > Building**. The Building Management page displays.

Step 2 Click on a building name.

Step 3 Click the **Feature Groups** tab.

Step 4 Click **Add**.

Caution Ensure that you are adding a Feature Group for the correct Building.

Step 5 Under Details, 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

- Check all the checkboxes that are relevant to the Unified CM release to which the Feature Group will be applied.

Step 6 Click **Submit**.

Note Repeat this for all required Features, and for all Customers.

This procedure updates BVSM.

Adding Customer, Division, and Shared Building Location Including VoiceMail and AutoAttendant Services

To create customers under Buildings, use the following steps:

Procedure

Step 1 **Choose General Administration > Resellers > Building > Customer** tab.

Step 2 Click Add.

Step 3 Click Add a new Customer.

Step 4 Click Add.

Step 5 To add a new location to an existing customer:

Step 6 Choose the **Add a new Location for an Existing Customer** option.

Step 7 Select the appropriate customer from the drop-down list box.

Note When you create customers by using this menu, it triggers a meta transaction that automatically creates division and location along with the customers. You can also add VoiceMail and AutoAttendant service pilot if VoiceMail and AutoAttendant services are already created in the Building.

Note You can set preferences at the building level for customers, divisions, and locations. If the preferences are set before you create the customer, division, and locations, then all new customer, division, location created will automatically be updated with the preference setting configured at the building level.

Use the following steps to change preferences in the building level:

Procedure

Step 1 Choose **Building > Preferences > Building Preferences** or **Default Customer Preferences** or **Default Location Preferences**.

These settings can be used to configure directory services, roaming login/logout features.

Step 2 Under **Details**, add the following:

- Name: <Customer Name>, for example: UKCustomer1
- Name: <Divison Name>, for example: UKCust1Div1
- Name: <Location Name>, for example: UKCust1Div1Loc1
- Country: <Country>, for example: UK
- TimeZone: <TimeZone>, for example: Europe/London
- Post/Zip Code: <Post/Zip Code>
- Contact Name: <ContactName>
- Contact Telephone Number: <ContactTelephoneNumber>

Step 3 Under Corporate Directory, add the following:

- IP Address <BVSMVirtualIP>, this is automatically provisioned.

Step 4 Click **Next >>**.

Step 5 Under Dial Plan Details, enter the following:

- Site Code: <LocSiteCode>, for example 111
- Select extension number length: <ExtLenght>, for example 4
- National Code: <DefAreaCode>, for example 1640

Step 6 Under Subnets, select IP Subnet assigned to Location <LocSubnet>; for example, 10.181.3.0

Step 7 Under Voice Mail Service, select appropriate VM service; for example, UKBuild1VMService1

Step 8 Under Auto Attendant Service, select appropriate AutoAttendant service; for example, UKBuild1AAService1

Step 9 Under Please select required Themes, perform the following tasks:

- Default branding of User Interface: Default GUI branding
- Tick the 'Default GUI branding' box

Step 10 Click **Next >>**.

Step 11 Under Enter number of lines required, enter the Required number of lines for each line type; for example, 500

Step 12 Under Enter the number of phones required, enter Required number of phones for each phone type; for example, 500

Step 13 Under Enter subscriber numbers for each service, enter the Required number of subscribers for each service; for example, 500

Note The number, line, and phone counters are not configured while creating a building. Once the building is created and during the creation if customer, divisions, locations the counter values from the reseller level is taken into account. So if there are not enough counter values reserved in the Reseller level, the counter values for the Shared building customers cannot be allocated.
Make sure there are enough counters (Number, line and Phone counters) reserved in the reseller level.

Step 14 Under Allowed Extension Ranges, enter the Ranges allocated for phones; for example, 300 - 400 (for three digit extensions) and 3000 - 4000 (for four digit extensions)

Under VoiceMail Service, enter the following:

- Voice Mail service name; for example, UKBuild1VMService1
- Select Pilot Number; for example, Extension Number 0010
- PSTN Number; for example, 16401110010

- Location VM Service Name; for example, UKBuild1VMPilot1

Under AutoAttendant Service, enter the following:

- Auto Attendant service name; for example, UKBuild1AAService1
- Select Pilot Number; for example, Extension Number 0011
- PSTN Number; for example, 16401110011
- Location AA Service Name; for example, UKBuild1AAPilot1

Step 15 Click **Add**.

This procedure updates BVSM, PGW, and Cisco Unified Communications Manager.

It is not mandatory to create Voicemail and Auto-Attendant pilots while creating building customer, division, locations. You can create the VoiceMail and AutoAttendant pilots from the Location menu. To do so, navigate to the shared building location **Advanced Management > VoiceMail Mgmt** or **Advanced Management > AutoAttendant Mgmt**.

To select Media services during location creation, add media service through **Resources > Media Services > Add**.

Moving Inventory of E164 Numbers and Phones to Shared Building Locations

This section describes the steps required to move the inventory of E164 numbers and Phones created at the provider level to customer locations.

IP Addresses (IP Subnets) created at the provider level are automatically associated with locations when the locations are created.

This section includes the following topics:

- Move E164 Number Inventory, page 10-14
- Move Phone Inventory, page 10-15

Caution Ensure that you are moving the Inventory of E164 Numbers and Phones to Locations at the correct Provider level.

Note To get to the Provider level, choose **Provider Administration > Providers**, and select a Provider.

Move E164 Number Inventory

To move a range of E164 Numbers to a Location, use the following procedure:

Procedure

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

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

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 : 1631clu1cus1loc1`
- Start of number Range: <startofnumberrange>; for example, 1631111000
- End of number Range: <endofnumberrange>; for example, 1631111019

Step 8 Click **Move**.

Note Repeat this for all required locations.

This procedure updates BVSM.

Move Phone Inventory

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

Procedure

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

Step 2 Select 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 Select a Move Target from the drop-down list box—<requiredlocation>; for example,

```
UKReseller1 : UKCustomer1 : UKDivision1 : 1631clu1cus1loc1
```

Step 5 Click **Next >>**.

Step 6 Select Subnet: <locationsubnet>; for example, 10.181.3.0

Step 7 Click **Move Phone**.

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

This procedure updates BVSM and Unified CM.

Caution The phone and a line will be added to the Unified CM, and the phone will register with the Unified CM , but the phone will have very restrictive settings. BVSM and the phone display will show as Unregistered.

Building Location Administration

This section describes the steps required to configure various location specific parameters; for example, the PSTN Published number, Emergency Published number, and so on. It also describes how to assign a range of E164 numbers to internal numbers, register phones, manage phones, add end users, manage end

users, add extension mobility, and add BVSM user roaming (Cross Cluster Forwarding that allows users to login/logout away from home Unified CM Cluster).

This section includes the following topics:

- Adding PSTN Published Number, page 10-16
- Adding Emergency Published Number, page 10-17
- Assigning Range of E164 Numbers to Internal Numbers, page 10-18
- Registering Phones, page 10-19
- Adding End User, page 10-20
- Adding User Extension Mobility, page 10-21
- Adding User Roaming (Cross Cluster Forwarding), page 10-22
- Managing Phones, page 10-24
- Managing User, page 10-24

Adding PSTN Published Number

If the PSTN Published number is configured, when a call from an IP Phone is destined to the PSTN (basic or call forwarded), the cgpn (and the redirecting number) will be replaced with the PSTN Published number. To add a PSTN Published Number:

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

Step 2 Click the name of the location to which you want to add the PSTN Published number.

Step 3 Click **Advanced Mgt**.

Step 4 Click **PSTN Published Number**.

Step 5 Under Details, enter the Published PSTN Number: <PSTNPubNumber>; for example, 1631111009.

Step 6 Click **Add**.

Note Repeat this for all required locations.

This procedure updates BVSM and PGW.

Adding Emergency Published Number

The Emergency Published number is required to correctly route emergency calls. When the Emergency Published number is configured, when an emergency calls is placed, the cgpn will be replaced with the Emergency Published number.

To add an Emergency Published Number, use the following steps:

Procedure

Step 1 Go to **General Administration > Locations**. Select a Location you want to add the Emergency Published number to.

Step 2 Click **Advanced Mgt**.

Step 3 Click **Emergency Number**.

Step 4 Emergency Number: <EmPubNum>, select an available E164 number; for example 1631111008

Step 5 Click **Add**.

Note Repeat this for all required locations.

This procedure updates BVSM and PGW.

Assigning Range of E164 Numbers to Internal Numbers

Note If the location requires PSTN calls to be routed via Local PSTN breakout, before proceeding with the provisioning steps in this section insure that:

- Location preference LocationCentralPSTNAccessOnly is disabled
- Location is connected to the relevant Local Gateway Interface

You can assign a range of E164 numbers for a range of internal extensions. These can then be assigned to an IP Phone, so that users can receive calls from the PSTN on those extensions.

To assign a Range of E164 numbers to internal numbers, use the following steps:

Procedure

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

Step 2 Click **Range Assoc**.

Step 3 Select a National Code—<NatCode>; for example, 1631.

Step 4 Click **Next >>**.

Step 5 Under Details, enter the following:

- For the Range Start
  - First PSTN Number in the range—<StartOfPSTNRange>; for example, 1631111000
  - First Extension Number in the range—<StartOfExtRange>; for example, 0200
- For the Range End:
  - Last PSTN Number in the range—<EndOfPSTNRange>; for example, 1631111019
  - Last Extension Number in the range—<EndOfExtRange>; for example, 0219

Step 6 Click **Submit**.

Note Repeat this procedure for all required locations.

This procedure updates BVSM and PGW.

Starting from Hosted UCS 6.1(a), BVSM 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.

Registering Phones

To Register a Phone, use the following steps:

Procedure

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

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

Step 3 Under Phone Features, enter the following:

- Phone Location: <PhoneLocation>; for example, Phone Switch 04 - Port1
- Select Phone Feature Group: <PhoneFeatureGroup>; for example, COS1International24Hour

Step 4 Click **Next >>**.

Step 5 Under 'Phone Details', enter the following:

- Softkey Template: <SoftkeyTemplate>; for example, Softkey_Advanced
- Device Use: <Phone or Fax>; for example, Phone

Under Number Details, enter the following:

- Line Number: <ExtOrE164>; for example, 1631111001
- Label: <PhoneLabel>; for example, Desk4

Step 6 Click **Register**.

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

This procedure updates BVSM and Unified CM.

Adding End User

To Add an End User, use the following steps:

Procedure

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

Step 2 Click **Add**.

Step 3 Under Details, enter the following:

- Username—<Username>; for example, clu1cus1loc1user1
- 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 Under Details, enter the following:

- Select the Extension from the drop-down menu—<ExtOrE164>; for example, 1631111002
- Label—<PhoneLabel>; for example, user1

Note You can add multiple lines, if required.

Step 6 Click **Add**.

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

This procedure updates BVSM and Unified CM.

Adding User Extension Mobility

You can set up Extension mobility to enable the user to log in to phones on its home Unified CM Cluster. To Add Extension Mobility for a User, use the following steps:

Procedure

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

Step 2 Click **Add** under Has Mobility, next to the user for whom you want to add extension mobility.

Step 3 Under User Mobility Profile, enter the following:

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

Under 'Number Details', enter the following:

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

Step 4 Click **Add**.

Note You can add multiple lines, if required.

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

This procedure updates BVSM and Unified CM.

Adding User Roaming (Cross Cluster Forwarding)

For a User with Extension Mobility, this feature enables Cross Cluster Forwarding to allow Users to login to phones away from their home Unified CM Cluster.

To activate this feature for providers, use the following steps:

Procedure

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 Check the checkbox to enable the user roaming setting.

Step 6 Click **Modify**.

Note Repeat this procedure for all required Providers.

To activate this feature for feature groups, use the following steps:

Procedure

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

Step 2 Select a Feature Group to be used by the User.

Step 3 Ensure that **User Mobility** and **Allow User login to Phone** are selected, and click **Modify**.

Note Repeat this procedure for all required Feature Groups.

To activate this feature for customers, use the following steps:

Procedure

Step 1 Choose **General Administration > Customers**. Select a Customer for whom 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 Check the available checkbox to enable the setting.

Step 9 Click **Modify**.

Note Repeat this procedure for all required customers.

Note BVSM now manages the Log-ins. Extension mobility is active if the User logs in to a phone in the home Unified CM Cluster, and Cross Cluster Forwarding is active if the user logs in to a phone that is away from home Unified CM Cluster.

This procedure updates BVSM and Unified CM.

Managing Phones

To Manage a Phone, use the following steps:

Procedure

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

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

This procedure updates BVSM and Unified CM.

You can use the Phone Management page to

- Reset the phone
- Login a user
- Logout a user
- Modify the Phone Button Template
- Modify the Phone Locale
- Delete Line(s)
- Modify Phone Features, for example EnableDisable PC Support, Enable/Disable Speaker, and so on
- Modify Line Settings, for example Enable/Disable Hot Line, Enable/Disable CallForwarding, and so on
- Unregister the Phone

Managing User

To Manage a User, use the following steps:

Procddure

Step 1 Go to **Location Administration > Users**.

Step 2 Select the phone you want to manage by clicking the MAC address of the phone; for example, clu1cus1loc1user1.

This procedure updates BVSM and Unified CM.

You can use the Users page to:

- Change the user password
- Change the user PIN
- Modify/Delete User Extension Mobility
- Associate the user to a Phone
- Delete the user

Note Be aware that the Shared Building feature does not support Legacy PBX.

CHAPTER 11

Provisioning Cisco Emergency Responder

This chapter describes enhanced emergency call routing using Cisco Emergency Responder (Cisco ER) via local gateways in the Hosted UCS reference architecture for Hosted Uunified Communications Services 6.1(a). The chapter also provides steps required to provision the enhanced Emergency Support feature via the VisionOSS BVSM application.

In the Hosted UCS architecture, by default, Emergency calls are sent to the PSTN with the Calling Party Number being replaced with the Location specific Emergency Published number. In Hosted UCS 6.1(a), Cisco Emergency Responder can be used to manage emergency calls in the telephony network so that it is possible to respond to these calls effectively and so that the service provider can comply with local ordinances concerning the handling of emergency calls. In North America, these local ordinances are called Enhanced 911 or E911. Other countries and locales might have similar ordinances. It is possible to provision some locations to handle emergency calls via the "Default" method, and provision others to use Cisco ER. For the Locations provisioned to use Cisco ER, Emergency calls are sent to the PSTN with the Calling Party Number being replaced with the Emergency Location Identification Number (ELIN) which enables the Public Safety Answering Point (PSAP) operator to correctly identify the location of the caller. It also enables the PSAP operator to callback the emergency caller.

Be aware that BVSM only provisions Unified CM and PGW to enable the correct routing of enhanced emergency calls and not Cisco ER. The Cisco ER server needs to be manually configured. This guide provides guidelines on when Cisco ER should be configured and which configuration should be applied to Cisco ER.

This chapter includes the following sections:

- Cisco Emergency Responder Integration, page 11-2

Cisco Emergency Responder Integration

This section provides a description of Cisco Emergency Responder integration into Hosted UCS.

This section covers the following topics:

- Planning for Cisco Emergency Responder Integration, page 11-2

Planning for Cisco Emergency Responder Integration

Before deploying Cisco Emergency Responder the Systems Integrator should obtain the following:

- PRI trunks to connect to the service provider. In Hosted UCS 6.1(a) CAMA trunks cannot be configured.
- Direct Inward Dial (DID) numbers for use as emergency location identification numbers (ELIN) for the emergency response locations (ERL).
- ALI Submission Requirements. 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. Besides routing the call appropriately, the ALI database also supplies the location information that appears on the PSAPs screens to help them locate the caller.

Note For further detals on planning for Cisco Emergency Responder, refer to the *Cisco Emergency Responder Administration Guide 2.0.*

Routing Emergency Calls in Hosted UCS without Cisco Emergency Responder

In the Hosted Unified Communications Services 6.1(a) architecture, if Cisco ER is not used to route Emrgency calls for a customer location, Emergency calls are sent to the PSTN with the Calling Party Number being replaced with the location specific Emergency Published Number.

The emergency call is routed in the following way:

1. User in Cluster 4 Customer 3 Location 1 Dials 911 - CdPN: 911; CgPN: 01400054310001 (DDI: 2124310001)

- Since the dialled digits are 911, the 911 Route Pattern is matched since it is associated with the AllowEmerCalls1 Partition, which in turn is in the EmergencyOnly1 Calling Search Space, which the Calling Search Space set for this device.
- On the 911 Route Pattern the CgPN is transformed using the 01400054431XXXX Calling Party Transformation Mask (which inserts the Emergency Call Type 4 after the CPIDRID) and the call is routed to the EMERGENCY1 Route List.
- On the EMERGENCY1 Route List the CdPN is prefixed with a 9, and send to the EXTERNAL Route Group.
- On the EXTERNAL Route Group the e4c1-External Trunk is configured, so the call is sent out of this trunk to the HSI.

Note The digit at the end of CSS Names, Partition Names, Route Pattern and Translation Pattern Names are used to set them as location specific.

2. Call is sent from Unified CM to the HSI - CdPN: 9911; CgPN: 014000544310001.

- No changes are made to the CgPN and CdPN numbers on the HSI.

3. Call is sent from HSI to the PGW over EISUP - CdPN: 9911; CgPN: 014000544310001.

- On the PGW the analysis starts in the ICCM dial plan:

```
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitst
ring="0140005",setname="GotoCust0009"
```

```
numan-add:resultset:custgrpid="ICCM",name="GotoCust0009"
numan-add:resulttable:custgrpid="ICCM",name="GotoCust0009",resultt
ype="NEW_DIALPLAN",dw1="0009",dw2="0",setname="GotoCust0009"
o   In the Customer 3 Ingress dial plan 0009:
numan-add:adigtree:custgrpid="0009",callside="originating",digitst
ring="01400054",setname="0140005siteE164emerg"
numan-add:digmodstring:custgrpid="0009",name="0140005siteE164emerg
",digstring="12124310009"
numan-add:digmodstring:custgrpid="0009",name="EmrgIndicator",digst
ring="99999"
numan-add:resultset:custgrpid="0009",name="0140005siteE164emerg"
numan-add:resulttable:custgrpid="0009",name="0140005siteE164emerg"
,resulttype="AMODDIG",dw1="1",dw2="99",dw3="0140005siteE164emerg",
dw4="0",setname="0140005siteE164emerg"
numan-add:resulttable:custgrpid="0009",name="InsertEmrgInd",result
type="BMODDIG",dw1="1",dw2="1",dw3="EmrgIndicator",setname="014000
5siteE164emerg"
numan-add:resulttable:custgrpid="0009",name="chg2CTRY",resulttype=
"NEW_DIALPLAN",dw1="CTRY",dw2="0",setname="0140005siteE164emerg"
o   In the CTRY dial plan:
numan-add:adigtree:custgrpid="CTRY",callside="originating",digitst
ring="1",setname="gotoN001"
numan-add:resultset:custgrpid="CTRY",name="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="setANoaIntl",resultty
pe="A_NUMBER_TYPE",dw1="5",setname="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="gotoN001",resulttype=
"NEW_DIALPLAN",dw1="N001",dw2="0",setname="gotoN001"
o   In the N001 dial plan:
numan-add:bdigtree:custgrpid="N001",callside="originating",digitst
ring="99999",setname="gotoEmergCountry1"
numan-add:resultset:custgrpid="N001",name="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="stripCC",resulttype="
AMODDIG",dw1="1",dw2="1",dw4="0",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="setANOA",resulttype="
A_NUMBER_TYPE",dw1="4",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="RmvEmergPrefix",resul
ttype="BMODDIG",dw1="1",dw2="5",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="EmergNoa",resulttype=
"B_NUMBER_TYPE",dw1="49",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="gotoEmergCountry1",re
sulttype="NEW_DIALPLAN",dw1="L001",dw2="1",setname="gotoEmergCount
ry1"
o   In the L001 dial plan:
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="2",setname="ToCentralGW"
numan-add:service:custgrpid="L001",name="l001afnt"
numan-add:resultset:custgrpid="L001",name="ToCentralGW"
```

```
numan-add:resulttable:custgrpid="L001",name="l001afnt",resulttype=
"NUM_TRANS",dw1="l001afnt",dw2="2",dw3="0",setname="ToCentralGW"
FNT entry: 1,l001afnt,2,2124310009,C0004C002124310009 is matched
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="C0004C00",setname="ToGw0004C00"
numan-add:digmodstring:custgrpid="L001",name="Gw0004C00",digstring
="0004C00"
numan-add:resultset:custgrpid="L001",name="ToGw0004C00"
numan-add:resulttable:custgrpid="L001",name="DeletePrefix",resultt
ype="AMODDIG",dw1="1",dw2="8",dw4="0",setname="ToGw0004C00"
numan-add:resulttable:custgrpid="L001",name="InsertPrefix",resultt
ype="BMODDIG",dw1="1",dw2="0",dw3="Gw0004C00",setname="ToGw0004C00
"
numan-add:resulttable:custgrpid="L001",name="ToLocalGW",resulttype
="NEW_DIALPLAN",dw1="LOGW",dw2="0",setname="ToGw0004C00"
o   In the LOGW dial plan:
numan-add:bnoa:custgrpid="LOGW",noavalue=49,setname="EnSCalls"
numan-add:resultset:custgrpid="LOGW",name="EnSCalls"
numan-add:resulttable:custgrpid="LOGW",name="BnoaUnk",resulttype="
B_NUMBER_TYPE",dw1="2",setname="EnSCalls"
numan-add:resulttable:custgrpid="LOGW",name="ToOffNetHSI",resultty
pe="ROUTE",dw1="rtlist2offnethsi",setname="EnSCalls"
```

4. Call is sent from PGW to Offnet HSI over EISUP - CdPN: 0004#00911; CgPN: 2124310009

- No changes are made to the CgPN and CdPN numbers on the OffNet HSI

5. Call is sent from Offnet HSI to the Local Gateway via H.323 - CdPN: 0004#00911; CgPN: 2124310009

- POTS dial-peer 99000400 is matched:

```
dial-peer voice 99000400 pots
 service hucstrans
 destination-pattern 0004#00T
 direct-inward-dial
 port 1/0/0:15
 no register e164
```

- 0004#00 is striped from the CdPN and the Local Gateway send the call to PSTN via PRI trunk

6. Call is sent to PSTN from Local Gateway via PRI - CdPN: 911; CgPN: 2124310009

Routing Emergency Calls in Hosted UCS with Cisco Emergency Responder

In Hosted UCS 6.1(a) Cisco ER can be used to manage emergency calls in the telephony network so that it is possible to respond to these calls effectively and so that the service provider can comply with local ordinances concerning the handling of emergency calls. In North America, these local ordinances are called Enhanced 911 or E911. Other countries and locales might have similar ordinances. It is possible to provision some locations to handle emergency calls via the Default method, and provision others to use Cisco ER. For the Locations provisioned to use Cisco ER, emergency calls are sent to the PSTN with the Calling Party Number being replaced with the Emergency Location Identification Number (ELIN) which enables the Public Safety Answering Point (PSAP) operator to correctly identify the location of the caller. It also enables the PSAP operator to callback the emergency caller.

The emergency call is routed in the following way:

1. User in Cluster 4 Customer 1 Location 1 Dials 911 - CdPN: 911; CgPN: 01400014110001 (DDI: 2124110001)

- Since the dialled digits are 911, the 911 Translation Pattern is matched since it is associated with the AllowEmerCalls12 Partition, which in turn is in the EmergencyOnly12 Calling Search Space, which is the Calling Search Space set for this device.
- On the 911 Translation Pattern a new CSS is selected: EUSACSS.
- The RP911 CTI Route Point (which is controlled by Cisco ER) is matched and the call is sent to Cisco ER.

2. Call is sent from Unified CM to the Cisco ER - CdPN: 911; CgPN: 01400014110001

- The IP Phone from which the Emergency call is initiated is associated with the Clu4Cus1Loc1-ERL1 Emergency Response Location. This ERL is configured with the 12129112211911 <--> 2129112211 Route Pattern <--> ELIN Number mapping. This means that 01400014110001 extension is mapped to the 2129112211 ELIN and the CdPN is transformed to 12129112211911. In addition to this the CERSec411-1 Onsite alert is associated with this ERL.

- The CERSec411-1 Onsite Alert is configured to call 01400014110000 which is the Internal number of the Onsite Security Phone for Cluster 4 Customer 1 Location 1.

3. Call is sent from Cisco ER to Unified CM - CdPN: 12129112211911; CgPN: 01400014110001

- On Unified CM 12129112211.911 Route Pattern is matched, since it is in the EUSACSS.
- On the 12129112211.911 Route Pattern the CgPN is transformed using the 014000142129112211 Calling Party Transformation Mask (which inserts the Emergency Call Type 4 after the CPIDRID and replaces SLCEXT with the ELIN), PreDot digits are removed from the CdPN and the call is routed to the EMERGENCY1 Route List.
- On the EMERGENCY1 Route List the CdPN is prefixed with a 9, and send to the EXTERNAL Route Group
- On the EXTERNAL Route Group the e4c1-External Trunk is configured, so the call is sent out of this trunk to the HSI.
- Cisco ER also calls the Onsite Security Phone for Cluster 4 Customer 1 Location 1 via one of the configured CTI Ports (99999990001) which are controlled by Cisco ER and play out the Emergency Message.

4. Call is sent from Unified CM to HSI over H.323 - CdPN: 9911; CgPN: 014000142129112211

- No changes are made to the CgPN and CdPN numbers on the HSI

5. Call is sent from HSI to PGW over EISUP - CdPN: 9911; CgPN: 014000142129112211

- On the PGW the analysis starts in the ICCM dial plan:

```
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitst
ring="0140001",setname="GotoCust0001"
numan-add:resultset:custgrpid="ICCM",name="GotoCust0001"
numan-add:resulttable:custgrpid="ICCM",name="GotoCust0001",resultt
ype="NEW_DIALPLAN",dw1="0009",dw2="0",setname="GotoCust0001"
o   In the Customer 1 Ingress dial plan 0001:
numan-add:adigtree:custgrpid="0001",callside="originating",digitst
ring="014000142129112211",setname="0140001siteELIN"
numan-add:digmodstring:custgrpid="0001",name="EmrgIndicator",digst
ring="99999"
numan-add:resultset:custgrpid="0001",name="0140001siteELIN"
numan-add:resulttable:custgrpid="0001",name="siteELINNoa",resultty
pe="A_NUMBER_TYPE",dw1="5",setname="0140001siteELIN"
```

```
numan-add:resulttable:custgrpid="0001",name="rmvCR4",resulttype="A
MODDIG",dw1="1",dw2="8",dw3="CCCountry1",dw4="0",setname="0140001s
iteELIN"
numan-add:resulttable:custgrpid="0001",name="InsertEmrg",resulttyp
e="BMODDIG",dw1="1",dw2="1",dw3="EmrgIndicator",setname="0140001si
teELIN"
numan-add:resulttable:custgrpid="0001",name="emergBNoa",resulttype
="B_NUMBER_TYPE",dw1="2",setname="0140001siteELIN"
numan-add:resulttable:custgrpid="0001",name="chng2CTRY",resulttype
="NEW_DIALPLAN",dw1="CTRY",dw2="0",setname="0140001siteELIN"
o   In the CTRY dial plan:
numan-add:adigtree:custgrpid="CTRY",callside="originating",digitst
ring="1",setname="gotoN001"
numan-add:resultset:custgrpid="CTRY",name="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="setANoaIntl",resultty
pe="A_NUMBER_TYPE",dw1="5",setname="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="gotoN001",resulttype=
"NEW_DIALPLAN",dw1="N001",dw2="0",setname="gotoN001"
o   In the N001 dial plan:
numan-add:bdigtree:custgrpid="N001",callside="originating",digitst
ring="99999",setname="gotoEmergCountry1"
numan-add:resultset:custgrpid="N001",name="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="stripCC",resulttype="
AMODDIG",dw1="1",dw2="1",dw4="0",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="setANOA",resulttype="
A_NUMBER_TYPE",dw1="4",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="RmvEmergPrefix",resul
ttype="BMODDIG",dw1="1",dw2="5",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="EmergNoa",resulttype=
"B_NUMBER_TYPE",dw1="49",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="gotoEmergCountry1",re
sulttype="NEW_DIALPLAN",dw1="L001",dw2="1",setname="gotoEmergCount
ry1"
o   In the L001 dial plan:
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="2",setname="ToCentralGW"
numan-add:service:custgrpid="L001",name="l001afnt"
numan-add:resultset:custgrpid="L001",name="ToCentralGW"
numan-add:resulttable:custgrpid="L001",name="l001afnt",resulttype=
"NUM_TRANS",dw1="l001afnt",dw2="2",dw3="0",setname="ToCentralGW"
FNT entry: 1,l001afnt,2,2129112211,C0000C012129112211 is matched
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="C0000C00",setname="ToGw0000C00"
numan-add:digmodstring:custgrpid="L001",name="Gw0000C00",digstring
="0000C00"
numan-add:resultset:custgrpid="L001",name="ToGw0000C00"
numan-add:resulttable:custgrpid="L001",name="DeletePrefix",resultt
ype="AMODDIG",dw1="1",dw2="8",dw4="0",setname="ToGw0000C00"
```

```
numan-add:resulttable:custgrpid="L001",name="InsertPrefix",resultt
ype="BMODDIG",dw1="1",dw2="0",dw3="Gw0000C00",setname="ToGw0000C00
"
numan-add:resulttable:custgrpid="L001",name="ToLocalGW",resulttype
="NEW_DIALPLAN",dw1="LOGW",dw2="0",setname="ToGw0000C00"
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="C0000C00",setname="ToGw0000C00"
o   In the LOGW dial plan:
numan-add:bnoa:custgrpid="LOGW",noavalue=49,setname="EnSCalls"
numan-add:resultset:custgrpid="LOGW",name="EnSCalls"
numan-add:resulttable:custgrpid="LOGW",name="BnoaUnk",resulttype="
B_NUMBER_TYPE",dw1="2",setname="EnSCalls"
numan-add:resulttable:custgrpid="LOGW",name="ToOffNetHSI",resultty
pe="ROUTE",dw1="rtlist2offnethsi",setname="EnSCalls"
```

6. Call is sent from PGW to Offnet HSI over EISUP - CdPN: 0000#00911; CgPN: 2129112211

- No changes are made to the CgPN and CdPN numbers on the Offnet HSI

7. Call is sent from Offnet HSI to the Local Gateway via H.323 - CdPN: 0000#00911; CgPN: 2129112211

- POTS dial-peer 99000000 is matched:

```
dial-peer voice 99000000 pots
 service hucstrans
 destination-pattern 0000#00T
 direct-inward-dial
 port 1/0/0:15
 no register e164
```

- 0000#00 is striped from the CdPN and the Local Gateway sends the call to PSTN via PRI trunk

8. Call is sent to PSTN from Local Gateway via PRI - CdPN: 911; CgPN: 2129112211

If both Cisco ER servers are not available or the Emergency call is initiated from an IP Phone which is un-allocated in Cisco ER, the call is routed to the PSAP operator servicing the Default ERL.

The emergency call is routed in the following way:

1. User in Cluster 4 Customer 1 Location 1 Dials 911 - CdPN: 911; CgPN: 01400014110001 (DDI: 2124110001)

- Since the dialled digits are 911, the 911 Translation Pattern is matched since it is associated with the AllowEmerCalls12 Partition, which in turn is in the EmergencyOnly12 Calling Search Space, which is the Calling Search Space set for this device.

- On the 911 Translation Pattern a new CSS is selected: EUSACSS.
- The RP911 CTI Route Point (which is controlled by Cisco ER) is matched but since the Primary Cisco ER Server is not available the call is forwarded to RP912 CTI Route Point (which is also controlled by Cisco ER) with the same CSS: EUSACSS.
- The RP912 CTI Route Point is matched but since Backup Cisco ER Server is not available the call is forwarded to 19999999999911 with the same CSS: EUSACSS.
- 19999999999.911 Route Pattern is matched since it is in the EUSA partition, which is in the EUSACSS.
- On the 19999999999.911 Route Pattern the CgPN is transformed using the #8#12128100098 Calling Party Transformation Mask (which replaces the CgPN with #8# + Country Code "1" + ELIN for the Default ERL), PreDot digits are removed from the CdPN and the call is routed to the EMERGENCY1 Route List.
- On the EMERGENCY1 Route List the CdPN is prefixed with a 9, and send to the EXTERNAL Route Group.
- On the EXTERNAL Route Group the e4c1-External Trunk is configured, so the call is sent out of this trunk to the HSI

2. Call is sent from Unified CM to HSI via H.323 - CdPN: 9911; CgPN: #8#12128100098

- No changes are made to the CgPN and CdPN numbers on the HSI

3. Call is sent from HSI to PGW over EISUP - CdPN: 9911; CgPN: #8#12128100098

- On the PGW the analysis starts in the ICCM dial plan:

```
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitst
ring="C8C",setname="ELINDefaultERL"
numan-add:digmodstring:custgrpid="ICCM",name="EmrgIndicator",digst
ring="99999"
numan-add:resultset:custgrpid="ICCM",name="ELINDefaultERL"
numan-add:resulttable:custgrpid="ICCM",name="ANOAInt",resulttype="
A_NUMBER_TYPE",dw1="5",setname="ELINDefaultERL"
numan-add:resulttable:custgrpid="ICCM",name="StripCPIDPlusOne",res
ulttype="AMODDIG",dw1="1",dw2="3",dw4="0",setname="ELINDefaultERL"
numan-add:resulttable:custgrpid="ICCM",name="InsertEmrgInd",result
type="BMODDIG",dw1="1",dw2="1",dw3="EmrgIndicator",setname="ELINDe
faultERL"
```

```
numan-add:resulttable:custgrpid="ICCM",name="chg2CTRY",resulttype=
"NEW_DIALPLAN",dw1="CTRY",dw2="0",setname="ELINDefaultERL"
```

- In the CTRY dial plan:

```
numan-add:adigtree:custgrpid="CTRY",callside="originating",digitst
ring="1",setname="gotoN001"
numan-add:resultset:custgrpid="CTRY",name="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="setANoaIntl",resultty
pe="A_NUMBER_TYPE",dw1="5",setname="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="gotoN001",resulttype=
"NEW_DIALPLAN",dw1="N001",dw2="0",setname="gotoN001"
```

- In the N001 dial plan:

```
numan-add:bdigtree:custgrpid="N001",callside="originating",digitst
ring="99999",setname="gotoEmergCountry1"
numan-add:resultset:custgrpid="N001",name="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="stripCC",resulttype="
AMODDIG",dw1="1",dw2="1",dw4="0",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="setANOA",resulttype="
A_NUMBER_TYPE",dw1="4",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="RmvEmergPrefix",resul
ttype="BMODDIG",dw1="1",dw2="5",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="EmergNoa",resulttype=
"B_NUMBER_TYPE",dw1="49",setname="gotoEmergCountry1"
numan-add:resulttable:custgrpid="N001",name="gotoEmergCountry1",re
sulttype="NEW_DIALPLAN",dw1="L001",dw2="1",setname="gotoEmergCount
ry1"
```

- In the L001 dial plan:

```
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="2",setname="ToCentralGW"
numan-add:service:custgrpid="L001",name="l001afnt"
numan-add:resultset:custgrpid="L001",name="ToCentralGW"
numan-add:resulttable:custgrpid="L001",name="l001afnt",resulttype=
"NUM_TRANS",dw1="l001afnt",dw2="2",dw3="0",setname="ToCentralGW"
numan-add:resulttable:custgrpid="L001",name="ToCentralGW",resultty
pe="NEW_DIALPLAN",dw1="F001",dw2="0",setname="ToCentralGW"
```

- In the F001 dial plan:

```
numan-add:bnoa:custgrpid="F001",noavalue=49,setname="EnSCalls"
numan-add:resultset:custgrpid="F001",name="EnSCalls"
numan-add:resulttable:custgrpid="F001",name="BnoaUnk",resulttype="
B_NUMBER_TYPE",dw1="2",setname="EnSCalls"
numan-add:resulttable:custgrpid="F001",name="ToPSTN",resulttype="R
OUTE",dw1="rtlist2pstn1",setname="EnSCalls"
```

4. Call is sent from PGW to Central PSTN Breakout via SS7 - CdPN: 911; CgPN: 2128100098

If a user makes an emergency call and the PSAP operator answers the call and after that the PSAP operator calls back, but then Cisco ER (the PSAP callback CTI Route Point) is unavailable, the call will be routed to the Default SP Onsite security, which will be the ELIN for the Default ERL.

If Cisco ER is not available when the PSAP operator callback is initiated, the call is routed in the following way:

1. PSAP operator (DDI: 2128911911) initaites callback to the emergency caller - CdPN: 2129112211; CgPN: 2128911911

- Call is sent from the PSTN to the Local Gateway via a PRI trunk.
- VOIP dial-peer voice 981 is matched:

```
dial-peer voice 981 voip
 translation-profile outgoing ToPGW
 destination-pattern ^1
 voice-class codec 1
 session target ras
 fax rate disable
 no vad
```

- CdPN is prefixed with #9#1 (here "1" is the country code).

2. Call is sent from Local Gateway to Offnet HSI via H.323 - CdPN: #9#12129112211; CgPN: 2128911911

- No changes are made to the CgPN and CdPN numbers on the HSI

3. Call is sent from Offnet HSI to the PGW over EISUP - CdPN: #9#12129112211; CgPN: 2128911911

- On the PGW the analysis starts in the ILGW dial plan:

```
numan-add:bdigtree:custgrpid="ILGW",callside="originating",digitst
ring="C9C1",setname="ToC1"
numan-add:resultset:custgrpid="ILGW",name="ToC1"
numan-add:resulttable:custgrpid="ILGW",name="stripCC",resulttype="
BMODDIG",dw1="1",dw2="4",setname="ToC1"
numan-add:resulttable:custgrpid="ILGW",name="BsetNOAnat",resulttyp
e="B_NUMBER_TYPE",dw1="4",setname="ToC1"
numan-add:resulttable:custgrpid="ILGW",name="ToP001",resulttype="N
EW_DIALPLAN",dw1="P001",dw2="1",setname="ToC1"
```

- In the P001 dial plan:

```
numan-add:anoa:custgrpid="P001",noavalue=4,setname="ANOAtoInt"
numan-add:resultset:custgrpid="P001",name="ANOAtoInt"
numan-add:resulttable:custgrpid="P001",name="changeNOA",resulttype
="A_NUMBER_TYPE",dw1="5",setname="ANOAtoInt"
```

```
numan-add:resulttable:custgrpid="P001",name="addCC",resulttype="AM
ODDIG",dw1="1",dw2="0",dw3="Country1CC",dw4="0",setname="ANOAtoInt
"
numan-add:bnoa:custgrpid="P001",noavalue=4,setname="BNOAtoInt"
numan-add:resultset:custgrpid="P001",name="BNOAtoInt"
numan-add:resulttable:custgrpid="P001",name="changeNOA",resulttype
="B_NUMBER_TYPE",dw1="5",setname="BNOAtoInt"
numan-add:resulttable:custgrpid="P001",name="addCC",resulttype="BM
ODDIG",dw1="1",dw2="0",dw3="Country1CC",setname="BNOAtoInt"
numan-add:resulttable:custgrpid="P001",name="gotoR001",resulttype=
"NEW_DIALPLAN",dw1="R001",dw2="1",setname="BNOAtoInt"
```

- In the R001 dial plan:

```
numan-add:bdigtree:custgrpid="R001",callside="originating",digitst
ring="12",setname="1rbpstnfnt"
numan-add:service:custgrpid="R001",name="r001bfnt"
numan-add:resultset:custgrpid="R001",name="1rbpstnfnt"
numan-add:resulttable:custgrpid="R001",name="rbpstnftn",resulttype
="NUM_TRANS",dw1="r001bfnt",dw2="1",dw3="49",dw4="ROUT",setname="1
rbpstnfnt"
FNT entry: 1,r001bfnt,1,12129112211,01400019112211 is matched
```

- In the ROUT dial plan:

```
numan-add:bdigtree:custgrpid="ROUT",callside="originating",digitst
ring="0140001",setname="gotoCustEgressDP0002"
o   In the Customer 1 Egress 2 dial plan:
numan-add:bdigtree:custgrpid="0002",callside="originating",digitst
ring="01400019112211",setname="CERPSAPCallback"
numan-add:digmodstring:custgrpid="0002",name="star",digstring="C"
numan-add:resultset:custgrpid="0002",name="CERPSAPCallback"
numan-add:resulttable:custgrpid="0002",name="Binsstar",resulttype=
"BMODDIG",dw1="4",dw2="0",dw3="star",setname="CERPSAPCallback"
numan-add:resulttable:custgrpid="0002",name="gotoH",resulttype="NE
W_DIALPLAN",dw1="H001",dw2="1",setname="CERPSAPCallback"
```

- In the H001 dial plan:

```
numan-add:adigtree:custgrpid="H001",callside="originating",digitst
ring="12",setname="AmodNat"
numan-add:digmodstring:custgrpid="H001",name="ninezero",digstring=
"91"
numan-add:resultset:custgrpid="H001",name="AmodNat"
numan-add:resulttable:custgrpid="H001",name="AmodNat",resulttype="
AMODDIG",dw1="1",dw2="1",dw3="ninezero",dw4="0",setname="AmodNat"
numan-add:bdigtree:custgrpid="H001",callside="originating",digitst
ring="0",setname="gotoHSI"
numan-add:resultset:custgrpid="H001",name="gotoHSI"
numan-add:resulttable:custgrpid="H001",name="Route2hsi",resulttype
="ROUTE",dw1="rtlist2hsi",setname="gotoHSI"
```

4. Call is sent from PGW to HSI over EISUP - CdPN: 014#00019112211; CgPN: 912128911911

- No changes are made to the CgPN and CdPN numbers on the HSI

5. Call is sent from HSI to Unified CM via H.323 - CdPN: 014#00019112211; CgPN: 912128911911

- The call enters Unified CM via e4c4-External trunk which is in the IncomingToCluster CSS. Since the EUSA Partition is in the IncomingToCluster CSS which is the configured partition of the 014#00019112211 Translation Pattern, this TP is matched.
- On the 014#00019112211 Translation Pattern the CdPN is transformed using the 9132129112211 Calling Party Transformation Mask and a new CSS is selected: EUSACSS.
- The RPELIN913 CTI Route Point (which is controlled by Cisco ER) is matched but since the Cisco ER Servers are not available the call is forwarded to 19999999999.2128100098 with the same CSS: EUSACSS.
- 19999999999.2128100098 Route Pattern is matched since it is in the EUSA partition, which is in the EUSACSS.
- On the 19999999999.2128100098 Route Pattern the CgPN is prexifed with #7#, PreDot digits are removed from the CdPN and the call is routed to the PSTNNAT1 Route List.
- On the PSTNNAT1 Route List the CdPN is prefixed with a 90, and send to the EXTERNAL Route Group.
- On the EXTERNAL Route Group the e4c1-External Trunk is configured, so the call is sent out of this trunk to the HSI

6. Call is sent from Unified CM to HSI via H.323 - CdPN: 902128100098; CgPN: #7#912128911911; RdN: 9132129112211

- No changes are made to the CgPN and CdPN numbers on the HSI

7. Call is sent from HSI to PGW over EISUP - CdPN: 902128100098; CgPN: #7#912128911911; RdN: 9132129112211

- On the PGW the analysis starts in the ICCM dial plan:

```
numan-add:adigtree:custgrpid="ICCM",callside="originating",digitst
ring="C7C",setname="CERDefOnsite"
numan-add:resultset:custgrpid="ICCM",name="CERDefOnsite"
numan-add:resulttable:custgrpid="ICCM",name="ANOAInt",resulttype="
A_NUMBER_TYPE",dw1="5",setname="CERDefOnsite"
```

```
numan-add:resulttable:custgrpid="ICCM",name="StripC7C9",resulttype
="AMODDIG",dw1="1",dw2="4",setname="CERDefOnsite"
numan-add:resulttable:custgrpid="ICCM",name="RemovePSTNAPx",result
type="BMODDIG",dw1="1",dw2="1",setname="CERDefOnsite"
numan-add:resulttable:custgrpid="ICCM",name="chg2CTRY",resulttype=
"NEW_DIALPLAN",dw1="CTRY",dw2="0",setname="CERDefOnsite"
numan-add:resulttable:custgrpid="ICCM",name="Strip913",resulttype=
"RMODDIG",dw1="1",dw2="3",dw4="0",setname="CERDefOnsite"
```

- In the CTRY dial plan:

```
numan-add:adigtree:custgrpid="CTRY",callside="originating",digitst
ring="1",setname="gotoN001"
numan-add:resultset:custgrpid="CTRY",name="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="setANoaIntl",resultty
pe="A_NUMBER_TYPE",dw1="5",setname="gotoN001"
numan-add:resulttable:custgrpid="CTRY",name="gotoN001",resulttype=
"NEW_DIALPLAN",dw1="N001",dw2="0",setname="gotoN001"
```

- In the N001 dial plan:

```
numan-add:bdigtree:custgrpid="N001",callside="originating",digitst
ring="0",setname="IntBgotoS001"
numan-add:digmodstring:custgrpid="N001",name="Country1CC",digstrin
g="1"
numan-add:resultset:custgrpid="N001",name="IntBgotoS001"
numan-add:resulttable:custgrpid="N001",name="IntB",resulttype="B_N
UMBER_TYPE",dw1="5",setname="IntBgotoS001"
numan-add:resulttable:custgrpid="N001",name="modBCC",resulttype="B
MODDIG",dw1="1",dw2="1",dw3="Country1CC",setname="IntBgotoS001"
numan-add:resulttable:custgrpid="N001",name="gotoS001",resulttype=
"NEW_DIALPLAN",dw1="S001",dw2="2",setname="IntBgotoS001"
```

- In the S001 dial plan:

```
numan-add:bdigtree:custgrpid="S001",callside="originating",digitst
ring="1",setname="switch2R001"
numan-add:resultset:custgrpid="S001",name="switch2R001"
numan-add:resulttable:custgrpid="S001",name="switch2R001",resultty
pe="NEW_DIALPLAN",dw1="R001",dw2="1",setname="switch2R001"
```

- In the R001 dial plan:

```
numan-add:bdigtree:custgrpid="R001",callside="originating",digitst
ring="12",setname="1rbpstnfnt"
numan-add:resultset:custgrpid="R001",name="1rbpstnfnt"
numan-add:resulttable:custgrpid="R001",name="rbpstnftn",resulttype
="NUM_TRANS",dw1="r001bfnt",dw2="1",dw3="49",dw4="ROUT",setname="1
rbpstnfnt"
numan-add:bdigtree:custgrpid="R001",callside="originating",digitst
ring="1",setname="switch2E001"
numan-add:resultset:custgrpid="R001",name="switch2E001"
numan-add:resulttable:custgrpid="R001",name="switch2E001",resultty
pe="NEW_DIALPLAN",dw1="E001",dw2="1",setname="switch2E001"
```

- In the E001 dial plan:

```
numan-add:adigtree:custgrpid="E001",callside="originating",digitst
ring="1",setname="SetNatANum"
numan-add:resultset:custgrpid="E001",name="SetNatANum"
numan-add:resulttable:custgrpid="E001",name="stripCC",resulttype="
AMODDIG",dw1="1",dw2="1",dw4="0",setname="SetNatANum"
numan-add:resulttable:custgrpid="E001",name="setANOA",resulttype="
A_NUMBER_TYPE",dw1="4",setname="SetNatANum"
numan-add:bdigtree:custgrpid="E001",callside="originating",digitst
ring="1",setname="toLocalGWNat"
numan-add:resultset:custgrpid="E001",name="toLocalGWNat"
numan-add:resulttable:custgrpid="E001",name="NatBNOA",resulttype="
B_NUMBER_TYPE",dw1="5",setname="toLocalGWNat"
numan-add:resulttable:custgrpid="E001",name="ToLocalGW",resulttype
="NEW_DIALPLAN",dw1="L001",dw2="1",setname="toLocalGWNat"
```

- In the L001 dial plan:

```
numan-add:adigtree:custgrpid="L001",callside="originating",digitst
ring="2",setname="ToCentralGW"
numan-add:resultset:custgrpid="L001",name="ToCentralGW"
numan-add:resulttable:custgrpid="L001",name="l001afnt",resulttype=
"NUM_TRANS",dw1="l001afnt",dw2="2",dw3="0",setname="ToCentralGW"
numan-add:resulttable:custgrpid="L001",name="ToCentralGW",resultty
pe="NEW_DIALPLAN",dw1="F001",dw2="0",setname="ToCentralGW"
```

- In the F001 dial plan

```
numan-add:bdigtree:custgrpid="F001",callside="originating",digitst
ring="12",setname="toNat"
numan-add:resultset:custgrpid="F001",name="toNat"
numan-add:resulttable:custgrpid="F001",name="BnoaNat",resulttype="
B_NUMBER_TYPE",dw1="4",setname="toNat"
numan-add:resulttable:custgrpid="F001",name="BstripCC",resulttype=
"BMODDIG",dw1="1",dw2="1",setname="toNat"
numan-add:resulttable:custgrpid="F001",name="ToPSTN",resulttype="R
OUTE",dw1="rtlist2pstn1",setname="toNat"
```

8. Call is sent from PGW to Central PSTN Breakout via SS7 - CdPN: 2128100098; CgPN: 2128911911; RdN: 2129112211

Provisioning Cisco Emergency Responder Integration

This section provides a description of the required provisioning steps in BVSM to integrate Cisco Emergency Responder into Hosted UCS. Since the Cisco ER servers are not provisioned by BVSM, some manual provisioning steps required on Cisco ER, LAN Switches, and Unified CM for the integration are also detailed. Following sections are included:

- Static Configuration, page 11-17
- Provisioning Cisco Emergency Responder Support, page 11-22

Static Configuration

This section details the initial static (manual) configuration required for Cisco ER Integration of the following Hosted UCS components:

- Cisco Emergency Responder Static Configuration, page 11-17
- LAN Switch Static Configuration, page 11-20
- Cisco Unified Communications Manager Static Configuration, page 11-20

Cisco Emergency Responder Static Configuration

This section includes the following topics:

- Configuring the SNMP Connection, page 11-17
- Identifying the LAN Switches, page 11-19

Configuring the SNMP Connection

Cisco ER uses SNMP to obtain information about the ports on a switch. Cisco ER must obtain this port information so that you can assign the ports to ERLs, and so that Cisco ER can identify phones that are attached to the ports and update their ERL assignments.

Cisco ER only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

Obtain the read community strings from all of the switches you will define in Cisco ER.

To configure the SNMP connection on Cisco ER, use the following steps.

Procedure

Step 1 Log into the Cisco Emergency Responder Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin; for example,

https://10.52.211.67/ceradmin.

Step 2 Choose Phone Tracking > SNMP Settings. On the SNMP Settings page, enter the following:

Step 3 Enter an 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 *.*.*.*. You will only need to create one entry. If subsets of your switches use the same strings, create a mask that covers those subsets, if possible. For simplicity, try to create the fewest number of patterns. If you use a separate string for each switch, you must enter each switch on this page.

Step 4 Enter the timeout and retries values. These values work together to determine how often and how long Cisco ER tries to obtain SNMP information from a switch before giving up.

Note The first attempt lasts as long as the timeout value. If you enter 1 or higher for retries, Cisco ER tries again, and each retry lasts twice as long as the previous try. For example, if you specify 10 for timeout, the first retry lasts for 20 seconds, the second retry lasts for 40 seconds, and so forth. The optimal values are 10 to 15 seconds for timeout, and 2 to 3 for retries.

Step 5 Enter the read community string; for example,CERGroup2.

Step 6 Click **Insert**.

Cisco ER adds the SNMP setting to the list of settings.

Identifying the LAN Switches

You must tell Cisco ER which switches it must manage. Cisco ER 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.

Because Cisco ER must obtain information from the switches, you must ensure that the information you supply to Cisco ER is correct and kept up-to-date. After you have created the initial switch list, you can make mass changes to switch definitions by exporting the switch definitions, editing the export file, and reimporting the file.

Caution Ensure that you configure the SNMP read community strings before adding switches.

To configure the LAN Switch on Cisco ER, use the following steps:

Procedure

Step 1 log into the Cisco Emergency Responder Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin; for example,

https://10.52.211.67/ceradmin.

Step 2 Choose **Phone Tracking > LAN Switch Details**.

Step 3 On the LAN Switch Details page, perform the following tasks:

- Enter the IP address or DNS name of the switch, for example 10.100.200.83
- Enter the Description, for example Desk 3 Phone Switch: IPCBU-PH-SW03
- Click **Insert** to add the switch to the Cisco ER configuration.

Step 4 Cisco ER asks if you want to run the switch-port and phone update process. You must run this process so that Cisco ER can identify the ports on the switch and so that your ERL administrator can then assign the ports to the right ERLs.

Note If you are adding more than one switch, you can skip running the process until you add the last switch. When you select to run the process, Cisco ER runs the process on all switches added since the last time the switch-port and phone update

process was run. If you do not choose to run the process, you can run it later by selecting **Phone Tracking > Run Switch-Port** and **Phone Update**.
In either case, newly discovered ports are assigned to the Default ERL.

LAN Switch Static Configuration

Cisco ER uses Cisco Discovery Protocol (CDP) to locate phones, so you should enable CDP on all of your switches. If you do not enable CDP, Cisco ER must use the Content Addressable Memory (CAM) table on the switch to track phones. Using the CAM table is less efficient than using CDP.

Cisco ER also uses SNMP to obtain information about the ports on a switch. Cisco ER must obtain this port information so that you can assign the ports to ERLs, and so that Cisco ER can identify phones that are attached to the ports and update their ERL assignments. Cisco ER only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

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

```
IPCBU-PH-SW03(config)#cdp run
IPCBU-PH-SW03(config)#snmp-server community CERGroup2 RO
```

Cisco Unified Communications Manager Static Configuration

When you configure the SNMP strings for the switches, you must also configure the SNMP strings for the Cisco Unified CM servers. Cisco ER must be able to make SNMP queries of all Cisco Unified CM servers in the cluster that it supports.

To configure the SNMP strings on Unified CM, use the following steps:

Step 1 Log into the Cisco Unified Communications Manager Serviceablility page:

https://<Unified_CM_IP_Address_or_name>/ccmservice.

Step 2 Choose **SNMP > V1/V2c > Community String**, and configure the following:

Step 3 From the Server drop-down list box, choose the server for which you want to configure a community string, for example 10.134.4.2

Step 4 Click **Add New**.

Step 5 In the Community String Name field, enter a name for the community string, for example: CERGroup2.

Step 6 From the Host IP Addresses Information group box, click the **Accept SNMP Packets only from these hosts** radio button.

Step 7 In the **Host IP Address** field, enter the IP addresses of the Primary Cisco ER server; for example,: 10.100.96.11 and click **Insert**.

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 To apply the community string to all nodes in the cluster, check the **Apply To All Nodes** check box.

Step 10 Click **Save**.

Step 11 A message indicates that changes will not take effect until you restart the SNMP master agent. To restart the SNMP master agent service, click **OK**.

Note For further details on SNMP configuration in Unified CM 5.x, refer to the SNMP V1/V2c Configuration section of the *Cisco Unified CallManager Serviceability Administration Guide*, Release 5.1(3).

Note For further details on SNMP configuration in Unified CM 6.X, go to the Configuring SNMP V1/V2c section of the *Cisco Unified Serviceability Administration Guide*, Release 6.1(1)

Provisioning Cisco Emergency Responder Support

This section provides a description of the required provisioning steps in BVSM in order to integrate Cisco Emergency Responder into Hosted UCS. Since the Cisco ER servers are not provisioned by BVSM, some of the sections provide the additional configuration steps required on Cisco ER. This section includes the following topics:

- Adding and Configuring Cisco ER Groups, page 11-22
- Adding Locations with Enhanced Emeergency Support, page 11-31
- Location Administration, page 11-32

Adding and Configuring Cisco ER Groups

There are several steps required to define and configure Cisco Emergency Responder Groups. The administrator needs to:

- Define Cisco ER Groups, page 11-22

Define Cisco ER Groups

To define a Cisco ER Group:

Procedure

Step 1 Choose **Network > Emergency Responder**.

Step 2 Click **Add**.

Step 3 Click **Add** next to CiscoEmergencyResponder.

Step 4 Under Cisco Emergency Responder Group Details, enter the following:

- Cisco Emergency Responder Group Name: <uniquename>, same as the Cisco ER Group Name configured in Cisco ER, for example CERGroup2 [see Note 1]
- Cisco Emergency Responder Group Description: <CERGroupdescription>, for example Cisco ER Group 2
- ELIN for Default ERL (Format: code-number): <ELINDefaultERL>, for example 2128100098

- Peer TCP Port: <PeerTCPPort>, for example 17001 [see Note 1]
- Heartbeat Count: <HeartbeatCount>, for example 3 [see Note 1]
- Heartbeat Interval (secs): <HeartbeatInterval>, for example 30 [see Note 1]
- Active Call Timeout (mins): <ActiveCallTimeout>, for example 180 [see Note 1]
- UDP Port Begin: <UDPPortBegin>, for example 32000 [see Note 1]
- Software Version: <CERVersion>, CiscoEmergencyResponder : Any
- Country: <CountrywhereCERis>, for example United States

Step 5 Check the **Detailed trace file of configuration sessions?** checkbox.

Step 6 Click **Next >>**.

Step 7 Under 'Primary Cisco Emergency Responder Details', enter the following:

- Host Name: <PrimaryCERHostName>; for example, IPCBU-CER3.

Note Currently, BVSM is not used to configure Cisco ER. The Cisco ER settings entered should correspond with the settings in Cisco ER. To verify the Cisco ER Group, Telephony, and Server Settings on Cisco ER, refer to "Verifying the Cisco Emergency Responder Group, Telephony, and Server Settings on Cisco Emergency Responder" section on page 11-24.

- Description—<PrimaryCERDescription>; for example, Primary Cisco ER Server
- IP Address—<PrimaryCERIPAddress>; for example, 10.100.96.12
- Config User Id—<CERSystemAdmin>; Intended for future use. This user should be part of the CER System Administrator user group; for example, CERAdministrator
- Config Password—<CERSystemAdminPassword>. Configure the CER System Administrator password; for example, ipcbuemea
- Route Point for Main Server—<RPforMainServer>; for example, 911

Step 8 Under BackupCisco Emergency Responder Details, enter the following:

Note This step is optional. If the secondary CER server is not installed, the Secondary Route Point will not be created in Unified CM, and the Call-Forwarding numbers of the the Primary Route Point will be configured with the Route Pattern for the Default ERL.

Step 9 Host Name—<SecondaryCERHostName>;for example; IPCBU-CER4

Step 10 Description—<SecondaryCERDescription>; for example, Secondary Cisco ER Server

Step 11 IP Address—<SecondaryCERIPAddress>; for example: 10.100.97.12

Step 12 Config User Id—<CERSystemAdmin>. This user should be part of the CER System Administrator user group; for example, CERAdministrator

Step 13 Config Password—<CERSystemAdminPassword>. Configure the CER System Administrator password; for example, ipcbuemea

Step 14 Route Point for Backup Server: <RPforMainServer>, for example: 912

Step 15 Click **Add**.

Note Repeat this for all required Cisco ER groups.

This procedure updates BVSM only.

Verifying the Cisco Emergency Responder Group, Telephony, and Server Settings on Cisco Emergency Responder

Currently BVSM is not used to configure Cisco ER. The Cisco ER settings entered should correspond with the settings in Cisco ER. To verify the Cisco ER Group, Telephony and Server Settings on Cisco ER, use the following steps:

Procedure

Step 1 Log into the Cisco Emergency Responder Administration page—

https://<Cisco_ER_IP_Address_or_name>/ceradmin; for example,

`https://10.52.211.67/ceradmin`.

Step 2 Choose **System > Cisco ER Group Settings**.

Step 3 On the Cisco ER Group Settings page, verify:

- Cisco ER Group Name
- Peer TCP Port
- Heart beat Count
- Heart Beat Interval (in sec)
- Active Call Time out (in min)

Step 4 Choose **Sytem > Telephony Settings**. On the Telephony Settings page, verify:

- UDP Port Begin

Choose **Sytem > Server Settings**. On the Server Settings page for the configured Cisco ER Group, verify:

- Host Name

Associate Cisco ER Groups with CUCM Clusters

To associate a Cisco ER Group with a Unified CM cluster, use the following steps:

Procedure

Step 1 Choose **Network > Emergency Responder**.

Step 2 Click **Connectivity** next to the Cisco ER Group you want to associate; for example, CERGroup2.

Step 3 Click **Emergency Responder=>PBX**.

Step 4 Select the Unified CM cluster you want to connect the Cisco ER Group to; for example, e4c4.

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, 9999901.

Note Ensure that the CTI Port numbers do not operlap with other configured Directory numbers, Extensions, and that they are non-dialable; for example, 9999901-9999910.

- Number of Telephony ports—<NumberofPorts>. Number of CTI Ports; for example, 10.

Step 7 Click **Connect**.

Note BVSM cannot provision the Cisco ER Cisco Unified CM user in Cisco Unified CM due to AXL API limitations. The administrator needs to manually create Cisco ER Cisco Unified CM user in Cisco Unified CM.

Craeting a Cisco Emergency Responder Cisco Unified Communications Manager User

To create a Cisco ER Cisco Unified CM user, use the following steps:

Procedure

Step 1 Log into the Cisco Unified CM Administration page:

https://<Unified_CM_IP_Address_or_name>/ccmadmin; for example,

https://10.52.211.144/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, ipcbuemea
- Confirm Password—<Password>. Re-enter the password; for example, ipcbuemea.

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 9999901-9999910 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**.

Step 7 Click the Standard CTI Enabled user group link to display the User Group configuration page.

Step 8 Click **Add Application Users to Group**. The Find and List Application Users pop-up window displays the list of application users.

Step 9 Click the checkbox next to the created user ID; for example, CERUser, and click **Add Selected**. Cisco Unified Communications Manager adds the selected user to the Standard CTI Enabled user group.

Note Currently BVSM is not used to configure Cisco ER; therefore you must identify one Cisco Unified Communications Manager server per Cisco Unified Communications Manager cluster that you want to manage with the Cisco ER group you are configuring. Cisco ER gets the list of phones registered with these Cisco Unified Communications Manager servers and tracks the movements of these phones.

Defining the Cisco Unified Communications Manager cluster on Cisco Cisco Emergency Responder

To define the Unified CM cluster on Cisco ER, use the following steps:

Procedure

Step 1 Log into the Cisco Emergency Responder Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin. for example :

https://10.52.211.67/ceradmin.

Step 2 Choose **Phone Tracking > Cisco Unified Communications Manager**.

Step 3 On the Cisco Unified Communications Manager page, enter the following:

- Cisco Unified Communications Manager—<CUCMName>. IP address or DNS name of the server; for example 10.134.4.2. This server must be running Cisco Unified Communications Manager and SNMP services. Do not define more than one Cisco Unified Communications Manager server within the same Cisco Unified Communications Manager cluster in the Cisco ER configuration.

- CTI Manager—<CTIManagerIP>. IP address or DNS name of the CTI manager for the cluster to which the server belongs;, for example, 10.134.4.2.
- CTI Manager User Name—<CERCUCMUser>, user created for Cisco Emergency Responder; for example, CERUser.
- CTI Manager Password—<CTIManPass>. User password; for example, ipcbuemea.
- Backup CTI 1 Manager—<BackupCTI1manager>. IP address or DNS name of the first backup CTI manager for the cluster.
- 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 you created for Cisco ER's use; for example, 9999901.
- Number of Telephony Ports—<NumberofPorts>. The number of CTI ports in the sequence you created for Cisco ER's use; for example, 10.

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.

Setting up the Default ERL

Currently, BVSM is not used to configure Cisco ER, therefore you must configure the Default ERL manually. The Default ERL should not be configured for any of the Switch Ports, Unlocated Phones, Manually Configured Phones or IP Subnets. The Default ERL is used internally by Cisco ER only if no other ERL is configured for that phone. Cisco ER also uses the Default ERL for all emergency calls when the Cisco ER server is first started (or restarted when there is no standby Cisco ER server) until the initial switch port update is finished (this process is started immediately). The ELIN should be an E.164 number that will route to the Service Provider network (additionally used if both Primary and Secondary CER servers in the CER group are not available).

To set up the default ERL, use the following steps:

Procedure

Step 1 Log into the Cisco Emergency Responder Administration page:

https://<Cisco_ER_IP_Address_or_name>/ceradmin; for example,

https://10.52.211.67/ceradmin.

Step 2 Choose **ERL > ERL Details**. Cisco ER opens the Find and List ERLs page.

Step 3 Click **Configure Default ERL**. Cisco ER opens the ERL Information for Default window.

Step 4 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
  1. log into the Cisco Unified CM Administration page: https://<Unified_CM_IP_Address_or_name>/ccmadmin, for example: https://10.52.211.144/ccmadmin.
  2. 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 Cisco ER, for example: 29999999999.911.
- ELIN—<ELINDefaultERL>. Number used in Section 3.2.1.1; for example, 2128100098.

Step 5 Configure the remaining required information as per the Setting Up the Default ERL section of the *Cisco Emergency Responder Administration Guide 2.0*.

Adding Created Cisco Emergency Responder Partition to the IncomingToCluster CSS

BVSM cannot add additional partitions to an existing CSS. Because of this, the administrator needs to manually add the created Cisco ER partition (for example EUSA), to the IncomingToCluster CSS.

To add the created Cisco ER partition (for example EUSA), to the IncomingToCluster CSS, use the following steps:

Procedure

Step 1 Log into the Cisco Unified CM Administration page:

https://<Unified_CM_IP_Address_or_name>/ccmadmin, for example:

https://10.52.211.144/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 Cisco ER 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.

Click **Save**.

Note Repeat this for all required Unified CMs you want to connect to this Cisco ER Group, and for all required Cisco ER Groups.

This procedure updates BVSM and Unified CM.

Add "CER-PGW-CUCM_Cluster" Hardware Group

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:

Procedure

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" Hardware Group
- Limit usage of this Harware 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.

Note Repeat this for all required Unified CMs connected to a Cisco ER Group, and for all required Cisco ER Groups.

Caution Ensure that only one Cisco ER group, PGW, and Unified CM cluster are selected in order for BVSM to provision the correct components.

This procedure updates BVSM only.

Adding Locations with Enhanced Emeergency Support

When a location that does not require Enhanced Emergency Support is created, two site specific route patterns (911 and 9.911) are added 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, two site specific translation patterns (911 and 9.911) are added to Unified CM which are used to detect emergency calls and route them to Cisco ER.

This procedure updates BVSM, Unified CM, and PGW.

Location Administration

This section describes the steps required to configure various location parameters, which are specific for Cisco ER support; for example, adding an Emergency Response Location (ERL) and adding an Emergency Line Identification Number (ELIN) to the ERL.

Caution Before proceeding with the provisioning steps in this section ensure that E.164 numbers to be used for ELINs have been added to BVSM, moved to the correct Location, associated to Internal numbers, and all phones are registered

This section includes the following topics:

- Add Emergency Response Location, page 11-32
- Add Emergency Line Identification Numbers to Emergency Response Location, page 11-33

Caution Ensure that you are administering the correct Location. The name of the Location will be shown on the screen,

Add Emergency Response Location

Depending on the requirements, a number of Emergency Response Locations (ERLs) can be associated to a location. For each of the ERLs created, a number of ELINs can be defined.

To add an ERL, use the following steps:

Procedure

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

Step 2 Click Emergency Response Location Management.

Step 3 Click **Add**.

Under Details, enter the following:

- Name: <ERLName>, for example Clu4Cus1Loc1-ERL1
- Description: <ERLDescription>, for example Clu4Cus1Loc1 Emergency Response Location 1
- Emergency Responder Hardware Group: <ERHwGroup>, for example cergr2-pgw4-e4c4-hwgrp

Step 4 Click **Submit**.

Note Repeat this procedure for all required locations.

This procedure updates BVSM only.

Add Emergency Line Identification Numbers to Emergency Response Location

For each of the created ERLs a number of ELINs can be defined.

To add an ELIN, use the following steps:

Procedure

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

Step 2 Click **Emergency Response Location Management**.

Step 3 Select an ERL you want to add an ELIN to; for example, Clu4Cus1Loc1-ERL1.

Step 4 Click **Add ELIN**.

Step 5 Select a DDI for the ELIN from the drop-down menu; for example, 212-9112201.

Step 6 Click **Submit**.

Currently BVSM is not used to configure Cisco ER, therefore you must configure the ERL and ELINs manually. An emergency response location (ERL) defines the area in which an emergency call is made. Security personnel and emergency response teams use ERL information to locate an emergency caller.

Note Before continuing with adding an ERL and ELINs to Cisco ER, review the additional requirements detailed in the Configuring Cisco Emergency Responder 2.0 chapter of *Cisco Emergency Responder Administration Guide 2.0*.

Setting up an Individual Emergency Response Location

To set up an Individual ERL, follow the steps detailed in the "Setting Up an Individual ERL and Its Automatic Location Information (ALI)" section of the Configuring Cisco Emergency Responder 2.0 chapter of *Cisco Emergency Responder Administration Guide 2.0*.

In Step 3 of this procedure, you must provide the following information:

- Under ERL Settings—ERL Name
- Under ELIN Settings—Route/Translation Pattern
- ELIN Number

The information you provide should correspond with the information in BVSM. To get this information from BVSM, use the following steps:

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 Clu4Cus1Loc1-ERL1.

Step 4 Under **Emergency Line Identification Numbers (ELINs)**, you will find the ELIN Settings:

- Line Number <ELINNumber>, for example 212-9112201
- Route Number <RoutePattern>, for example 22129112201.911

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.

Note For further details on how to assign switch ports to ERLs, refer to the Configuring Cisco Emergency Responder 2.0 chapter of *Cisco Emergency Responder Administration Guide 2.0*:

Note Repeat this procedure for all required ERLs and for all required locations.

This procedure updates BVSM, PGW and Unified CM.

CHAPTER 12

Provisioning Cisco Unified Contact Center Hosted Integration

This chapter describes the required steps to configure the Cisco Unified Contact Center Hosted (UCCH) Integration feature introduced with Cisco Hosted Unified Communications Services (UCS), Release 6.1(a).

Since the Cisco UCCH components are not provisioned by BVSM, static configuration is required. Also, as the integration is not totally automated, some manual configuration is also required.

This chapter includes the following sections:

- Provisioning Cisco Unified Contact Center Hosted feature
- Static/manual Configuration

Provisioning Cisco Unified Contact Center Hosted feature

This section provides a description of the required provisioning steps in BVSM to integrate Cisco Unified Contact Center Hosted (UCCH) into Cisco Hosted UCS.

It includes:

- Configuring CUCM Application User and PG User

Configuring CUCM Application User and PG User

CUCM Application Users and PG users are used to connect Peripheral Gateways to CUCM. A preliminary static configuration step is required. See Static/manual Configuration on how to configure Application Users in CUCM and PG Users in Peripheral Gateways.

Following this preliminary step, you can proceed to the BVSM provisioning procedures as described in the following sections:

- Adding and Configuring Cisco CVP and VXML gateway
- Adding Contact Center pilot numbers (pre-routing calls)
- Contact Center Agents Administration
- Provisioning HUCS for additional options (Post-routing calls, Cisco IP IVR)

Adding and Configuring Cisco CVP and VXML gateway

There are several steps required to define and configure Cisco Customer Voice Portal. The administrator needs to:

- Define Cisco Customer Voice Portal
- Connect Cisco Customer Voice Portal to Transit switch
- Define VXML gateway

The following procedures require an already provisioned country dial plan.

Define Cisco Customer Voice Portal

To define a Cisco Customer Voice Portal, perform the following steps:

Procedure

Step 1 Go to **Network > Contact Centre**.

Step 2 Click **Add**.

Step 3 In the CC server Details, enter the following:

- Hostname: <*uniquename*>, for example enter CC1-CVP1 for the first CVP server of the first Contact Center system or enter the actual hostname of the CVP server.
- Description: <*CCdescription*>, for example CVP1 of Contact Center 1.
- IP address: <*CC IP address*>, enter the CVP IP address; for example for city 8 CC 10.120.8.80

Note The IP address is just a parameter for BVSM as BVSM does not configure the CVP.

- Country code: <*CC country code*>, for example, `United Kingdom`

Note The country you specify here will be used in the next step from the CONNECT operation to connect the Contact Center to the R<countrycode> PGW dial plan (for example for UK it will be the R044 dial plan).

- CPID: <*CCCPID*>, enter one of the CPID available or select AUTO; for example, `123`
  This number is the technology prefix that must be configured on the CVP server; the CVP server will use it to register to the gatekeeper.

Step 4 Click **Add**.

Connect Cisco Customer Voice Portal to Transit switch

Logically it should be more appropriated to connect it to a gatekeeper but in the actual BVSM implementation it has to be connected directly to the Transit Switch.

To connect the CVP to transit switch (PGW), perform the following steps:

Procedure

Step 1 Go to **Network > Contact Center**.

Step 2 Click the Contact Center server you need to connect; for example, `CC1-CVP1`

Step 3 Click **Connect**. PGW dial plan connected to the R<*country code*> dial plan as specified in Configuring Application User in CUCM.

Step 4 Choose the Transit Switch to connect to and click **Connect** correspondingly.

Step 5 Do a manual configuration; see Configuring Application User in CUCM.

Define VXML gateway

VXML gateways are defined in the same way as CVP servers. The following procedure helps to allocate CPID for VXML gateway and prevent further usage from BVSM; VXML gateway does not need to be connected to a Transit Switch;

To define a VXML gateway, perform the following steps:

Procedure

Step 1 Go to **Network > Contact Centre**.

Step 2 Click **Add**.

Step 3 In the CC server Details, enter the following:

- Hostname: <*CCservername*>, for example enter CC1-VXMLgw1 for the first VXML gateway of the first Contact Center system or enter the actual hostname of the CVP server.
- Description: <*CCdescription*>, for example VXML gateway 1 of Contact Center 1.

- IP address: <*CC IP address*>, enter the CVP IP address; for example, `10.120.8.80`
- Country code: <*CC country code*>, for example, `United Kingdom`
- CPID: <*CCCPID*>, enter one of the CPID available or select AUTO; select for example, `124`; this number will be the technology prefix that needs to be configured on the VXML gateway. The VXML gateway will use it to register to the gatekeeper.

Step 4 Click **Add**.

Step 5 Do a manual configuration; see Configuring PG User in Peripheral Gateway

Adding Contact Center pilot numbers (pre-routing calls)

Contact Center Pilot numbers are provisioned into the PGW in order to route the call to the ICM system through the CVP.

This section includes the following:

- Define Contact Center Service
- Add Pilot Number

Define Contact Center Service

To define a contact center service, perform the following steps:

Procedure

Step 1 Go to **Resources > Contact Centre Service**.

Step 2 Click **Add**.

In the CC service Details, enter the following:

- CC Service Name: <*CCservicename*>, for example, `CC1-CVP1-service1` for the first Contact Center service associated to first CVP of the first ICM system in the CVP1-ICM1.
- Description: <*CC service description*>, for example, `service 1 - CVP1 - Contact Center system 1`

- CC server: <*CCserver*>, select the corresponding CC server; for example, `CC1-CVP1`

Note Always select a CVP server, never select a VXML gateway.

- CC service ID: <*CC service ID*>, ID corresponding to the RID; select AUTO or one of the available ID.

Note CC service ID is only used internally in BVSM.

Step 3 Click **Add**.

Add Pilot Number

To add a pilot number, perform the following steps:

Procedure

Step 1 Go to **Resources > Contact Centre Service**.

Step 2 Click the CC service you want to associate pilot numbers. For example, `CC1-CVP1-service1`

Step 3 For Pilot Numbers, click **Add Pilot Number**

Step 4 For CC Service Pilot Number Details, enter the following:

- Pilot Number: <*CCpilotnumber*>, enter the pilot number. See Note.
- Description: <*CCpilotnumberdescription*>, enter a description, usually refer to the Customer assigned to the pilot number. For example, CC pilot number 1 - customer 1 - CC1-CVP1-service1

Step 5 Click **Add**.

Note The pilot number you enter should follow the international E.164 number format (Country Code plus E.164 number) without the leading "+" (or "00").

For example,
For the UK E.164 number 01640111001 that corresponds to the international E.164 number +441640111001 (Country Code=0044), enter **441640111001**

For the US number +12008000111 (Country Code=001), enter **2008000111**

For an incoming call to Contact Center, pilot numbers are sent from the PGW to the CVP in the format entered (prefixed with the CPID) and they are not transformed in FINT format; for example if you enter 441640111001 and the associated Contact Center service has CPID=123, the number sent to the CVP in the H323 message is 123#441640111001.
As the CPID is equal to the tech-prefix of the CVP, the CVP will strip the CPID and then will send the pilot number to the ICM (that is the same number entered into BVSM).

Contact Center Agents Administration

This section describes the steps required to configure Contact Center Agent lines.

You can configure two different types of agent lines:

- Agent lines associated to IP phones (standard agent lines)
- Agent lines associated to Roaming profiles (extension mobility agent lines)

Caution Before you start to provision agent lines, it is necessary to define the Contact Center tag.

The following sections include:

- Define Contact Center tag
- Standard Agent Lines
- Extension Mobility Agent Lines (roaming profiles))

Define Contact Center tag

This is the tag that Unified CCMP uses when it retrieves lines information (Directory numbers information) from CUCM; CCMP will use this information to associate the line to the Contact Center system.

This parameter is not a per-customer parameter but is a global parameter.

To define the Contact Center tag, perform the following steps:

Procedure

Step 1 Go to **Setup Tools > Global Settings**.

Step 2 Click **CClineprefix**.

Step 3 For Details, enter the following:

- Current settings: <*CClineprefix*>, for example, `CC_label`

Note Once you configure and begin the Agent Line provisioning, ensure not to change this value further.

Step 4 Click **Modify**.

Standard Agent Lines

This section describes how to provision standard agent lines associated to the IP phones.

It includes the following:

- Provision of standard Agent Line
- Manage of Standard Agent Line (add/remove)

Provision of standard Agent Line

Standard lines are lines directly associated to IP phones.

To register an IP phone, perform the following steps:

Procedure

Step 1 Go to **Location Administration > Phone Registration**.

Step 2 Click the MAC address of the phone to select the phone you want to register. For example, `001D452CDA84`

Note The IP phone that the agent uses must be associated to the Application User used by the ICM system. This procedure must be done manually.

Step 3 In the Phone Features, enter the following:

1. Phone Location: <*PhoneLocation*>, for example, `Phone Switch 04 - Port1`
2. Select Phone Feature Group: <*PhoneFeatureGroup*>, for example, `COS1International24Hour`
3. Click **Next**.

Step 4 In the Phone Details, enter the following:

- Softkey Template: <*SoftkeyTemplate*>, for example, `Softkey_Advanced`
- Device Use: <*Phone or Fax*>, for example, `Phone`

In the Number Details, enter the following:

- Line Number: <*ExtOrE164*>, for example, `1631111001`
- Label: <*PhoneLabel*>, for example, `Desk4`
- Check the Contact Center Agent lines checkbox. This check box becomes available when a Contact Center tag is defined.

Step 5 Click **Register**.

Repeat this for all required phones with associated Agent Lines, and for all required Locations.

Manage of Standard Agent Line (add/remove)

You can add or remove Agent lines to existing IP phones with an associated line.

To do this, perform the following steps:

Procedure

Step 1 Go to **Location Administration > Phone Management**.

Step 2 Click the username to select the phone you want to manage. For example, `001D452CDA84`

Note The IP phone of the agent must be associated to the Application User used by the ICM system.

Step 3 In the Settings (per Line), check or uncheck the Contact Centre Agent Line checkbox on the corresponding line. This is done to set/unset the line as a Contact Center line [see Note 2]

Note This check box becomes available when a Contact Center tag is defined. Checking it makes BVSM provisioning the CUCM with a modified line description field.

Step 4 Click **Modify**.

Extension Mobility Agent Lines (roaming profiles)

This section describes how to provision agent lines associated with roaming profiles.

It includes the following sections:

- Extension Mobility Agent Lines
- Manage Extension Mobility Agent Lines (add/remove)

Extension Mobility Agent Lines

Extension mobility agent lines are associated in BVSM to mobility users.

Add User Extension Mobility is the step used to provision the standard Agent line.

To add extension mobility with an associated Contact Center line, perform the following steps:

Procedure

Step 1 Go to **Location Administration > Users**.

Step 2 In 'Has Mobility', click **Add** corresponding to the user for which you want to add extension mobility.

Step 3 In the User Mobility Profile, 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`

Note IP phones in which agents will log-in, need to be associated to Application User used by the ICM system.

Step 4 In the Number Details, enter the following:

- Select the Extension from the drop-down menu: <*ExtOrE164*>, for example, `DDI 1631111002`
- Label: <*PhoneLabel*>, for example, `user1`
- Check the checkbox Contact Center Agent lines.

Note This checkbox becomes available when a Contact Center tag is defined. Checking this checkbox makes BVSM provisioning the CUCM with a modified line description field.

Step 5 Click **Add**.

Repeat this for all required Users, and for all required Locations.

Manage Extension Mobility Agent Lines (add/remove)

You can add or remove Agent lines to existing extension mobility users roaming with an associated line.

To do this, perform the following steps:

Procedure

Step 1 Go to **Location Administration > Users**.

Step 2 Click the name of the specific User.

Go to **Roaming Profile**:

In Line Features, check/uncheck the Contact Centre Agent Line checkbox on the corresponding line. This is done to set/un-set the line as a Contact Center line.

Note This check box becomes available when a Contact Center tag is defined.

Step 3 Click **Modify**.

Provisioning HUCS for additional options (Post-routing calls, Cisco IP IVR)

Following sections are included for additional options:

- Route-points for post-routing calls
- Cisco IP IVR

Route-points for post-routing calls

The creation of route point and associated DN is not automated. Using BVSM it is possible to define numbers/FINTs that should be used in the manual configuration to associate a DN to the CUCM route point.

You must allocate an internal number for every Agent associated to a location. Normally this number does not need to be routable from the PGW. The agent uses the EXTN associated to their location in order to make a call using the route point.

In case the number needs to be routable, the internal number needs to be associated to an E.164 number.

To create route points in BVSM, perform the following steps:

Procedure

Step 1 Go to **Location Administration > Internal Numbers**.

Step 2 Choose the internal number and click either **Prevent/Reserve**; for example, prevent the usage of the number 100.

Step 3 Identify the corresponding FINT number (CPID+RID+SLC+EXTN) and the site number of the Location. This is required for the manual configuration.

Step 4 In order to identify the FINT number:

- CPID code: Select a cluster in PBX devices/CCM cluster management to retrieve it; for example, the number retrieved is 010.
- RID code: Select a Location in Location/Manage Location to retrieve it; for example, the number retrieved is 0010.
- SLC (site code): Select a Location in Location/Manage location to retrieve it; for example, the number retrieved is 411.
- EXTN is the internal number (100).

Step 5 To identify the Site number of the Location, go to **General Administration > Locations** and select the Location.

Step 6 Go to Advanced Management and pick up the Location Identifier value; for example `1`.

Step 7 Proceed with the manual configuration. See Create CTI ports and associated DNs for every customer IP IVR.

Cisco IP IVR

Cisco IP IVR is not integrated in HUCS through the BVSM automation; also Cisco IP IVR configures entries in CUCM by itself.

Using BVSM it is possible to define numbers/FINTs that should be used in manually configuring CTI ports and CTI route points.

An internal number is allocated for every location with Agents.

To do this, perform the following steps:

Procedure

Step 1 In BVSM, go to **Location Administration > Internal Numbers**.

Step 2 Choose the internal number and click either **Prevent/Reserve**. For example, prevent the usage of the number 950.

Step 3 Identify the corresponding FINT number (CPID+RID+SLC+EXTN) and the site number of the Location; this is required for the manual configuration.

Step 4 In order to identify the FINT number:

- CPID code: Select a cluster in PBX devices/CCM cluster management to retrieve it; for example, the number retrieved is 010.
- RID code: Select a Location in Location/Manage Location to retrieve it; for example, the number retrieved is 0010.
- SLC (site code): Select a Location in Location/Manage location to retrieve it; for example, the number retrieved is 411.
- EXTN is the internal number (950).

Step 5 In order to identify the Site number of the Location, go to **General Administration > Locations**, and select the Location.

Step 6 Go to Advanced Management and pick up the Location Identifier value; for example `1`

Step 7 Repeat the procedure for any CTI route point/CTI port number needed (for example 950 will be the number for the CTI route point and 902, 903, 904…..909 will be the numbers for CTI ports).

Step 8 Proceed with the manual configuration. See Create CTI ports and associated DNs for every customer IP IVR.

Static/manual Configuration

This section details the static (manual) configurations required for Cisco Unified Contact Center Hosted (UCCH) integration.

It includes the following:

- Configuring CUCM Application User and PG User
- Configure CVP and VXML gateway for HUCS
- Associate phone to application user
- Create route-point and associated DNs (post-routing calls)
- Create CTI ports and associated DNs (Cisco IP IVR)

Configuring CUCM Application User and PG User

This section includes the following:

- Configuring Application User in CUCM
- Configuring PG User in Peripheral Gateway

Configuring Application User in CUCM

A CUCM cannot be shared from agents of different customers. So a customer (Contact Center enabled) requires their own Application User on the CUCM.

To configure an Application User in CUCM, perform the following steps:

Procedure

Step 1 Login to the Publisher CUCM.

Step 2 From the CallManager Administration window, go to User Management.

Step 3 Go to **Application User > Add a New User**.

The User Information window appears.

Step 4 In the UserID field, enter the User ID, and in the User Password field, enter the password.

The values must match the JTAPI user and password value that is entered in the PG User in the ICM Setup (see Configuring PG User in Peripheral Gateway).

For example, enter the User ID: `usr-pg1a-acd1`

Step 5 Add the group Standard CTI enabled.

Step 6 Fill the other required fields.

Step 7 Click **Save**.

Configuring PG User in Peripheral Gateway

In order to configure the CUCM Application User into the Peripheral Gateway, perform the following steps:

Procedure

Step 1 Run the ICM setup.

Step 2 In Cisco ICM setup:

- Select ICM instance of the customer (for example, `Customer1`)
- Select Peripheral Gateway Instance component (for example, `PG1`) and click **Edit**.

Step 3 In Peripheral Gateway properties, edit the PIM allocated for the CUCM or Add a new one;

Note Please refer to the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1).*

Step 4 In the CallManager Configuration dialog box, to put the PIM into service, check the Enabled checkbox.

This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

Step 5 In the Peripheral name field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name). For example, `e8c4s1`

Step 6 In the Peripheral ID field, from the Peripheral record, enter the Peripheral ID value from the Configuration Manager (use the PG Explorer tool to view the Peripheral ID). For example, `5000`

Step 7 In the Agent extension length field, enter the number of digits used (the maximum value is 15). This must match the length of FINT numbers. For example, `13`

Step 8 In the Service field, enter the hostname or the IP address of the machine that is running the Cisco CallManager software. If you use the hostname, the name must be in the hosts file. For example, `10.134.8.2`

Step 9 In the User ID field, enter the User ID entered for the PG on the Cisco CallManager Administrator web page (as created previously in Configuring Application User in CUCM when you added the PG as a new user). For example, `usr-pg1a-acd1`

Step 10 In the User password field, enter the User Password entered for the PG on the Cisco CallManager Administrator web page as created previously (see Configuring Application User in CUCM).

Step 11 In the Mobile Agent Codec drop-down list, select a codec value. For example, `G.711`

Step 12 Complete the setup.

Configure CVP and VXML gateway for HUCS

Following sections are included:

- Configuring CVP for HUCS
- Configuring VXML gateway for HUCS

Configuring CVP for HUCS

To configure the CVP for HUCS, perform the following steps:

Procedure

Step 1 Run the Voice Browser Administration located in C:\Cisco\CVP\bin\VBAdmin.bat.

Step 2 On the Voice Browser Administration, set the gatekeeper IP address and the zone; use the command **`setgk`** <*IP address*>. For example, to set the IP address 10.120.8.1 and the zone HUCS_ZONE:

```
setgk 10.120.8.51:HUCS_ZONE
```

Note To register within the gatekeeper default zone, use the command: **`setgk 10.120.8.51`**

Step 3 To set the tech-prefix registered to the gatekeeper, use the command **`settechprefix`** <*tech-prefix*>.

For example to set the tech-prefix 123#:

```
settechprefix 123#
```

The new setting will be updated upon system startup.

Note CVP looks for the first # and strips all the characters before; so it is not possible to use the tech-prefix #123#.

Configuring VXML gateway for HUCS

To configure the VXML gateway using IOS commands, perform the following steps:

Procedure

Step 1 Configure the CVP server; IP address or name of the Customer Voice Portal server; for example, `10.120.8.80 (E8CVP1A)`

Step 2 Configure the HUCS gatekeeper; IP address or name of the gatekeeper; for example, `10.120.8.51 (GLK2600-ENT8A)`

Step 3 Configure the HUCS gatekeeper zone; name of the HUCS zone; for example: HUCS_ZONE

Step 4 Configure the Media server; IP address or name of the media-server; for example in the case the CVP is used as a media-server too: 10.120.8.80 (e8cvp1a)

Step 5 Configure the DNS server; if name resolution is necessary, configure the DNS server; for example, configure the I address of the DNS server E8AD1: 10.131.8.100.

An example of a VXML Gateway configuration:

Following is an example of the IOS configuration of a VXML Gateway:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CVPGW-ENT8
!
boot-start-marker
boot system flash:c5400-js-mz.124-15.T4.bin
no boot startup-test
boot-end-marker
!
no logging console
enable password cisco
!
!
!
resource-pool disable
no aaa new-model
spe default-firmware spe-firmware-1
!
!
ip cef
ip domain name icm8.ipcbuemea.com
ip host isn-vxml 10.120.8.80
ip host isn-server 10.120.8.80
ip host mediaserver 10.120.8.80
ip host cvpserver 10.120.8.80
ip host cvpmedia 10.120.8.80
ip name-server 10.131.8.100
!
```

```
!
multilink bundle-name authenticated
!
!
voice service voip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback none
 h323
  h225 timeout setup 5
!
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
!
!
voice class h323 1
  call start slow
!
!
!
!
!
!
!
!
application
  service vru-leg flash:bootstrap.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
  !
  service new-call flash:bootstrap.vxml
  paramspace english index 0
```

```
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
  !
  service handoff flash:handoff.tcl
  paramspace english language en
  paramspace english index 0
  paramspace english location flash
  paramspace english prefix en
  !
!
!
!
archive
 log config
  hidekeys
!
!
controller E1 6/0
!
controller E1 6/1
!
controller E1 6/2
!
controller E1 6/3
!
controller E1 6/4
!
controller E1 6/5
!
controller E1 6/6
!
controller E1 6/7
!
controller E1 7/0
```

```
!
controller E1 7/1
!
controller E1 7/2
!
controller E1 7/3
!
controller E1 7/4
!
controller E1 7/5
!
controller E1 7/6
!
controller E1 7/7
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.120.8.100 255.255.255.0
 duplex full
 speed 100
 negotiation auto
 h323-gateway voip interface
 h323-gateway voip id HUCS_ZONE ipaddr 10.120.8.51 1719
 h323-gateway voip h323-id CVPGW-ENT8
 h323-gateway voip tech-prefix 124#
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 negotiation auto
!
```

```
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
 no fair-queue
!
interface Serial6/0
 no ip address
 shutdown
!
interface Serial7/0
 no ip address
 shutdown
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Group-Async0
 no ip address
 encapsulation slip
 group-range 1/00 5/107
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.120.8.1
!
no ip http server
!
!
logging trap debugging
logging facility local0
!
!
!
```

```
!
control-plane
!
!
!
!
!
dial-peer voice 100 voip
 service vru-leg
 incoming called-number 124#.
 dtmf-relay h245-signal h245-alphanumeric
 codec g711ulaw
 no vad
!
!
gateway
 timer receive-rtp 1200
!
ss7 mtp2-variant Bellcore 0
ss7 mtp2-variant Bellcore 1
ss7 mtp2-variant Bellcore 2
ss7 mtp2-variant Bellcore 3
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 60 0
 password cisco
 login
line 1/00 4/59
 modem InOut
line 5/00 5/107
 modem InOut
!
scheduler allocate 10000 400
```

```
ntp clock-period 17180026
ntp server 10.100.100.2
end
```

Note You can configure a technology prefix defined for the VXML-GW with the character #. So it is possible to configure a technology prefix like #124#.

Associate phone to application user

The IP phones used by agents need to be associated to the application user (the one corresponding to the PG User for that cluster/subscriber).

To associate IP phones to the Application User, perform the following steps:

Procedure

Step 1 Login to the Publisher CUCM interface.

Step 2 From the CallManager Administration window, go to **User Management > Application User**.

Step 3 Select an application user. For example, `usr-pg1a-acd1`

The User Information window appears.

Step 4 In the Device Information area, associate the IP phones as Controlled Devices; for example, associate it as: `SEP0017E0340BB2`

Step 5 Click **Save**.

Create route-point and associated DNs (post-routing calls)

For post-routing calls, you must identify the route points to ICM. While making a post-route call, you must dial the CTI route point associated DN numbers.

Perform the following three operations:

1. Create CTI route points (at least one for each customer)
2. Associate DN (lines) to the CTI route point
3. Associate CTI route points to Application User

Create CTI route points

To create a CTI route point from the CallManager Administration window, perform the following steps:

Procedure

Step 1 Choose **Device > CTI Route Point**.

Step 2 To add a new CTI route point, click **Add New**.

The CTI Route Point Configuration window appears.

Step 3 Enter the Route Point name in the Device Name field. For example, `cc_pg1a_411_rp`

Note Follow this naming convention. While naming CTI ports or Route Points use the following leading characters:
CTI route point names with leading "rpcc" or "RPCC"
CTI route point names with leading “cc” or "CC"

Step 4 Enter a brief description in the Description field.

Step 5 Select the Device Pool drop-down list. Select for example, `DevicePool1 for Location Identifier 1`

Step 6 Enter the Calling Search Space. For example, `COS1International 24hours` for Location Identifier 1.

Step 7 Enter the Location. For example, `location-BVSM-1 for Local Identifier 1`

Step 8 Click **Save**.

Associate DN (lines) to the CTI route point

To associate the directory number (this number has to be in FINT format), perform the following steps:

Procedure

Step 1 Add a new DN to the CTI Route Point.

Step 2 Enter the number in the Directory Number field. For example, `0100010411100`

Note In the example, CPID=010, RID=0010, SLC=411 EXTN=100.

Step 3 Select the Route Partition from the drop-down list. For example, `Site1` for Location Identifier 1.

Step 4 Select the Calling Search Space from the drop-down list. For example, `COS1International 24hours` for Location Identifier 1.

Step 5 Click **Save**.

Associate CTI route points to Application User

In the CUCM Administration window, perform the following steps:

Procedure

Step 1 Go to **User Management > Application User**.

Step 2 Select an application user. For example, `usr-pg1a-acd1`

Step 3 In the Device Information area, associate the CTI route point as Controlled Devices. For example, associate it as: `cc_pg1a_411_rp`

Step 4 Click **Save**.

Create CTI ports and associated DNs (Cisco IP IVR)

This section provides guidelines on how to connect Cisco IP IVR to HUCS-CUCCH.

Note Refer to the *Cisco IPCC Configuration Guides* for details on how to configure a Cisco IP IVR in an ICM system.

The IP IVR communicates with the CUCM through Java Telephony Application Programming Interface (JTAPI), and the IP IVR communicates with the ICM through the Service Control Interface (SCI) with an IVR Peripheral Gateway.

Configure the CUCM from the Cisco IP IVR itself; the Cisco IP IVR will use the AXL SOAP transaction to configure the CUCM. So you must provide the AXL SOAP user credentials on the Cisco IP IVR server. Cisco IP IVR will configure the following in the CUCM:

1. Create Application User for every customer IP IVR (with “CTI enabled” capabilities)
2. Create CTI ports and associated DNs for every customer IP IVR
3. Create CTI route points (IVR triggers) and associated DNs for every customer IP IVR
4. Associate CTI route points and CTI ports to the IP IVR application user for every customer IP IVR

Create Application User

This operation is done through the Cisco IP IVR during the creation of the JTAPI user.

Create CTI ports and associated DNs for every customer IP IVR

To create a JTAPI Call Control Group on CRS, login to the Cisco IP IVR and go to the CRS Administration window.

Perform the following steps:

Procedure

Step 1 Go to Subsystems/Unified CM Telephony.

Step 2 Select Add a New Unified CM Telephony Call Control Group.

Step 3 Enter the Group ID. For example, `1`

Step 4 Enter the Number of CTI ports. The number of CTI ports that need to be created; for example, `8`

Step 5 Enter the Starting Directory Number. CTI Ports numbers must correspond to the ones configured on BVSM; for example `0100010411902` to configure 8 ports with DNs 0100010411902, 0100010411903, 0100010411904, …….. 0100010411909

Note In this example, CPID=010, RID=0010, SLC=411 EXTN=902, 903, 904.

Step 6 In the Device Name prefix, configure the prefix you will use, in order to configure CTI ports in the CUCM. For example `z` or `cc`

Note When naming CTI ports or Route Points, use the following leading characters (use the single character ‘z” or “Z” for any problem with the length):
"rpcc" or "RPCC" for routepoint
"cc" or "CC" for routepoint
"ivr" or "IVR" for routepoint
"ipivr" or "IPIVR" for routepoint
"cc" or "CC" for CTI ports
"z" or "Z" for CTI ports
"ivr" or "IVR" for CTI ports
"ipivr" or "IPIVR" for CTI ports

Step 7 Device Pool is related to the Location Identifier. Select for example `DevicePool1` for Location Identifier 1.

Step 8 Calling Search Space is related to the Location Identifier. Select for example `COS1International 24hours` for Location Identifier 1.

Step 9 Location is related to the Location Identifier. Select for example `location-BVSM-1` for Local Identifier 1.

Step 10 Partition is related to the Location Identifier. Select for example `Site1` for Location Identifier 1

Create CTI route points (IVR triggers) and associated DNs for every customer IP IVR

To configure the Cisco ICM translation routing, perform the following steps:

Procedure

Step 1 Go to Applications/Application Management and Add a New Application.

Step 2 Choose as Application type: Cisco ICM translation-routing

Step 3 Enter the name; for example, `TransRouteCl4`

Step 4 Enter a unique ID. This field corresponds to the service identifier of the call reported to the Cisco ICM and configured in the Cisco ICM translation route. For example, `7000`

Step 5 Add a new trigger to the translation route.

To add a new trigger:

Step 6 Choose Unified CM telephony trigger.

Step 7 Set the directory number; this is the number associated to the CTI route point; this number must correspond to the one configured on BVSM; for example, `0100010411950`

Note In this example, CPID=010, RID=0010, SLC=411 EXTN=950.

Step 8 Set the Call Control Group Unified: select Unified CM Telephony Group #1(1) (refer to the previously created JTAPI call control group).

Step 9 On the Device Name, configure the name of the CTI Route Point. For example, `IP IVR1Atrigger`

Note When naming CTI ports or Route Points, use the following leading characters (use the single character ‘z” or “Z” for any problem with the length):
"rpcc" or "RPCC" for routepoint
"cc" or "CC" for routepoint
"ivr" or "IVR" for routepoint
"ipivr" or "IPIVR" for routepoint
"cc" or "CC" for CTI ports
"z" or "Z" for CTI ports
"ivr" or "IVR" for CTI ports
"ipivr" or "IPIVR" for CTI ports

Step 10 Device Pool is related to the Location Identifier. Select for example `DevicePool1` for Location Identifier 1.

Step 11 Calling Search Space is related to the Location Identifier. Select for example `COS1International 24hours` for Location Identifier 1.

Step 12 Location is related to the Location Identifier. Select for example `location-BVSM-1` for Local Identifier 1.

Step 13 Partition is related to the Location Identifier. Select for example, `Site1` for Location Identifier 1

CHAPTER 13

Provisioning Other Hosted Unified Communications Services Features

This chapter describes how to use VisionOSS Business Voice Services Manager (BVSM) application to provision the components of the Cisco Hosted Unified Communications Services (UCS), Release 6.1(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) 6.1(a) deployment.

This chapter includes the following sections:

- Provider Specific Features
- Customer Specific Features
- Location Specific Features
- Phone Specific Features

Provider Specific Features

Cisco Hosted Unified Communications Services, Release 6.1(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 6.1(a) environment.

This section contains:

- Forced Central PSTN Breakout
- Forced OffNet

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 BVSM 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
- Allowed To Use

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 6.1(a) extends support to the Forced OffNet facility.

It allows you to configure the Cisco PGW using BVSM 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 6.1(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 BVSM interface to provision “Forced” Central PSTN Breakout.

After upgrading to Cisco Hosted UCS 6.1(a), the Administrator must re-provision the previously configured numbers using the provisioning procedure as described in Forced Central PSTN Breakout.

Customer Specific Features

This section describes the steps required to configure customer specific features in a Cisco Hosted UCS 6.1(a) environment.

Cisco Hosted UCS 6.1(a) supports the Block OffNet To OffNet Transfer (BO2OT) customer specific feature.

It is possible to configure a customer using BVSM, 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
- Configure BO2OT for Specific Customers
- Configure BO2OT for Customers in a Building

Note Ensure to mark all Unified CM Route Patterns for all locations provisioned in Cisco Hosted UCS 6.1(a) as OffNet, instead of OnNet.

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 Go to **Network > PBX Devices**.

The Manage PBX Server window appears.

Step 2 Select one of the Unified CM clusters where customer locations are provisioned.

The CCM Cluster Management window appears.

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

The Import/Refresh CCM Items window appears.

Step 4 Check the Service Parameters checkbox and click **Import**.

The Manage PBX Server window appears.

Step 5 Once the transaction is successful, click **Return to Manage PBX Server**.

Step 6 Select the Unified CM cluster again.

Step 7 Click **Attributes**.

Step 8 Check the required BlockOffNetToOffNetTransfer parameter option and click **Modify**.

Repeat this procedure for all Unified CM clusters where customer locations are provisioned.

Note The next procedure is to configure specific customers using the BO2OT facility. If you are part of a shared building, to continue provisioning, you can skip to the Configure BO2OT for Customers in a Building section.

Configure BO2OT for Specific Customers

To provision a specific customer to Block OffNet To OffNet Transfers, perform the following steps:

Procedure

Step 1 Go to **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. It displays the name of the reseller. For example, `Configuring BOSOT for Customer - BVSM administrator at the Reseller level - UKReseller1`

Step 3 Click **Advanced Mgt.**.

The Advanced Customer Management window appears.

Step 4 Click **Advanced Telephony Settings**.

Step 5 Click **Enable or Disable** (based on the requirement).

Repeat this procedure for all customers who require this feature.

Configure BO2OT for Customers in a Building

For shared buildings, BO2OT is enabled at the building level and hence all customers hosted by the building will have blocked offnet to offnet transfers.

To provision a specific building to Block OffNet To OffNet Transfers, perform the following steps:

Procedure

Step 1 Go to **General Administration > Buildings**.

Step 2 Select the building you want to configure, from the Search Results area.

Caution Ensure that you are configuring buildings for the correct reseller. It displays the name of the reseller. For example, `Configuring BOSOT for Shared Building - BVSM administrator at the Reseller level - UKReseller1`

The Building Management window appears.

Step 3 Click **Advanced Mgt.**.

The Advanced Building Management window appears.

Step 4 Click **Advanced Telephony Settings**.

Step 5 Click **Enable** to enable the Block OffNet To OffNet Transfer, or even vice versa, based on the requirement.

Repeat this procedure for all buildings that require this feature.

Location Specific Features

This section describes the steps required to configure location specific features in a Cisco Hosted UCS 6.1(a) environment.

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
- NPA Geographic Split

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).

Overlay Area Codes are defined in BVSM as Adjacent Area Codes.

To add an Overlay Area Code, perform the following steps:

Procedure

Step 1 Go to **General Administration > Locations**.

Step 2 Choose a provider from the Search Results area.

Step 3 Choose an appropriate customer from the Customer Management window.

Step 4 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. It displays the name of the location. For example, `Overlay Area Codes - BVSM administrator at the Location level – 212clu2cus1loc1`

Step 5 The Manage Location window appears.

Step 6 Click **Advanced Mgt.**.

Step 7 Click **Adjacent Area Codes**.

Step 8 Click **Add**.

Step 9 For Enter Adjacent Area Code, enter <OverlayAreaCode>, for example `646`

Step 10 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 6.1(a) environment.

Support for XML Phone Application was tested for the first time on Hosted UCS 6.1 (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
- Add XML Phone Service to a Feature Group
- Personalize phone with XML Application

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**.

APPENDIX A

Hosted Unified Communications Services Location Administration

This document describes the options available to Location-level administrators within the Hosted UCS system, Release. 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, page A-1
- Quick Search, page A-2
- Transactions (General Tools), page A-6
- Hunt Groups, page A-6
- Line Groups, page A-10
- Pickup Groups, page A-12
- Users, page A-16
- Phone Registration, page A-24
- Phone Management, page A-26
- Extensions, page A-28

Note For information about using the options on the Self Care menu, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b)*.

User Interface Guidelines

Note the following conventions used in these menus and associated administration pages:

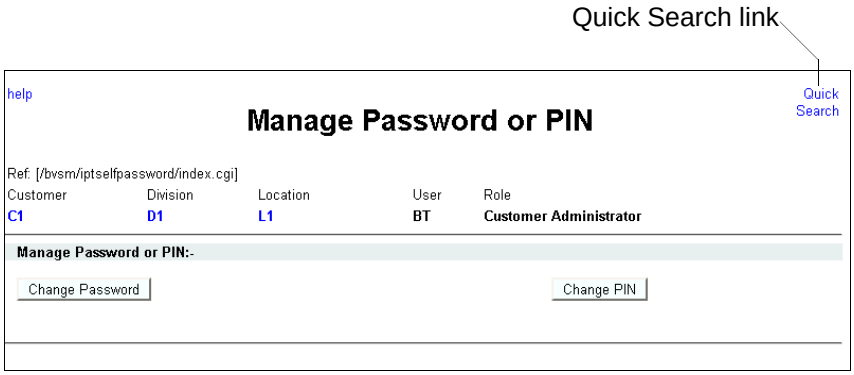
- Links to other pages are bright blue.
- Required fields are indicated by a red asterisk (*).
- Error messages are displayed in red type.
- Most changes provide a transaction record that indicates if the transaction is successful and that may provide an explanation if it is not.

- 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

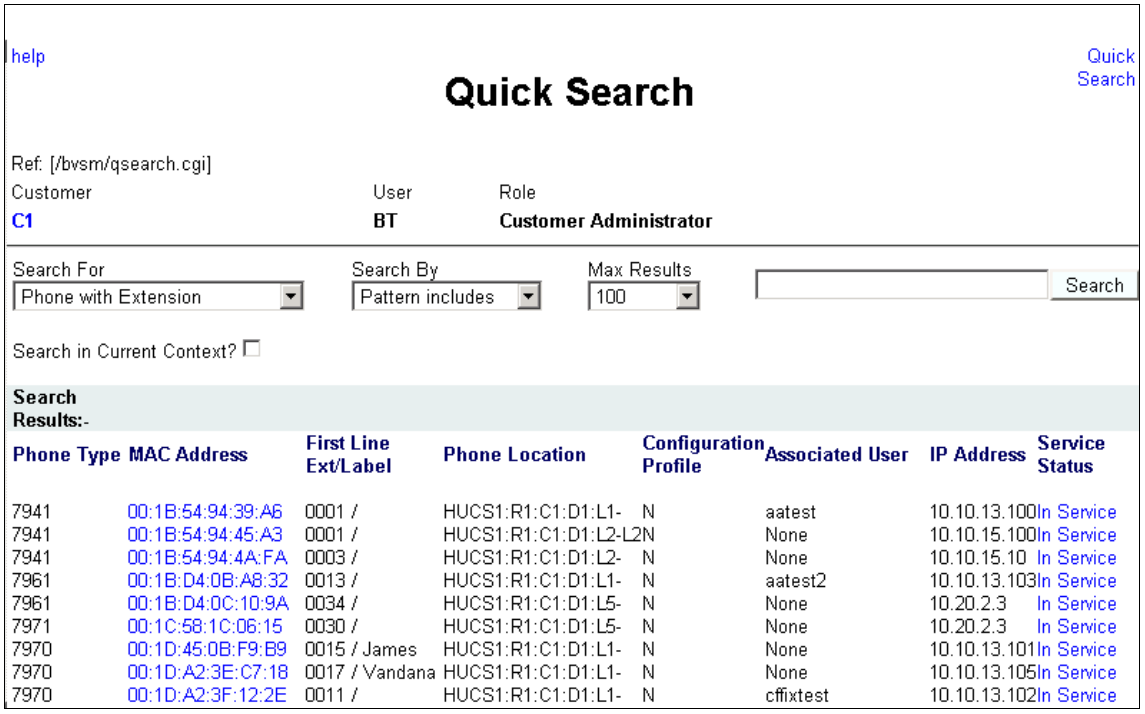
As shown in Figure A-1, each page of the BVSM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries 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.

Table A-1 Search Types

Search Type	Description
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- 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 BVSM 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 BVSM 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 BVSM.

4. Associate a phone to a user account (once associated, the user account will be listed in the corporate directory).

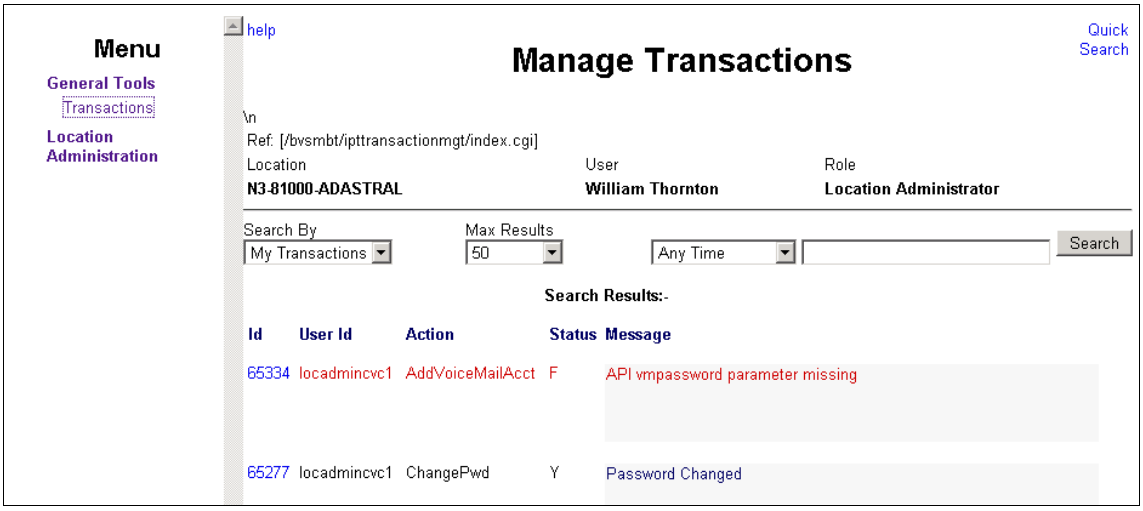
This step is performed at the location level from the User Management page for the location.

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 "Line Groups" section on page A-10. 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.

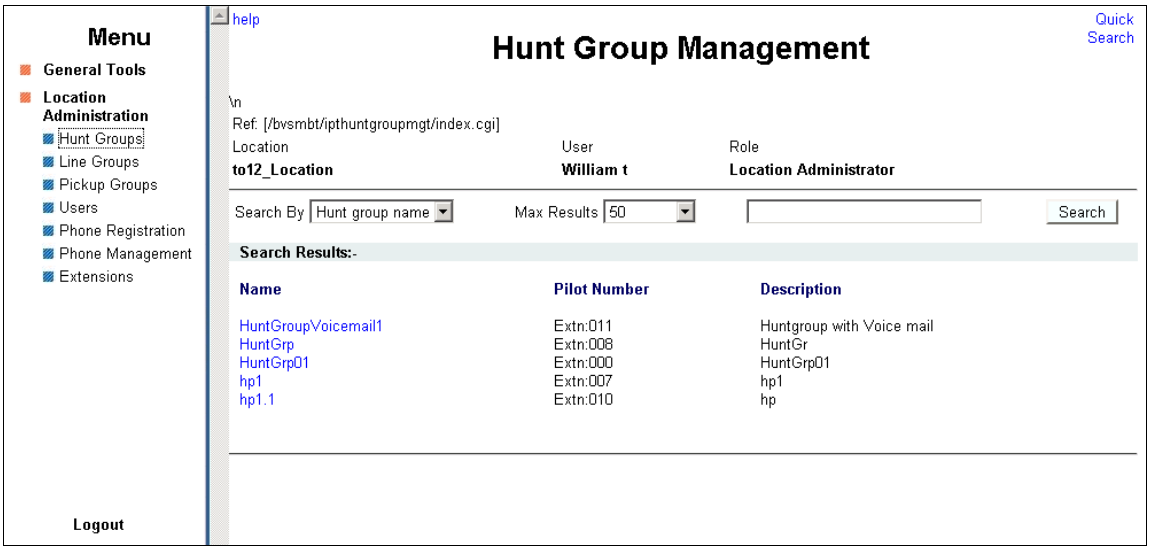
To configure the Maximum Hunt Timer or Call Forward Destination, complete the following steps:

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

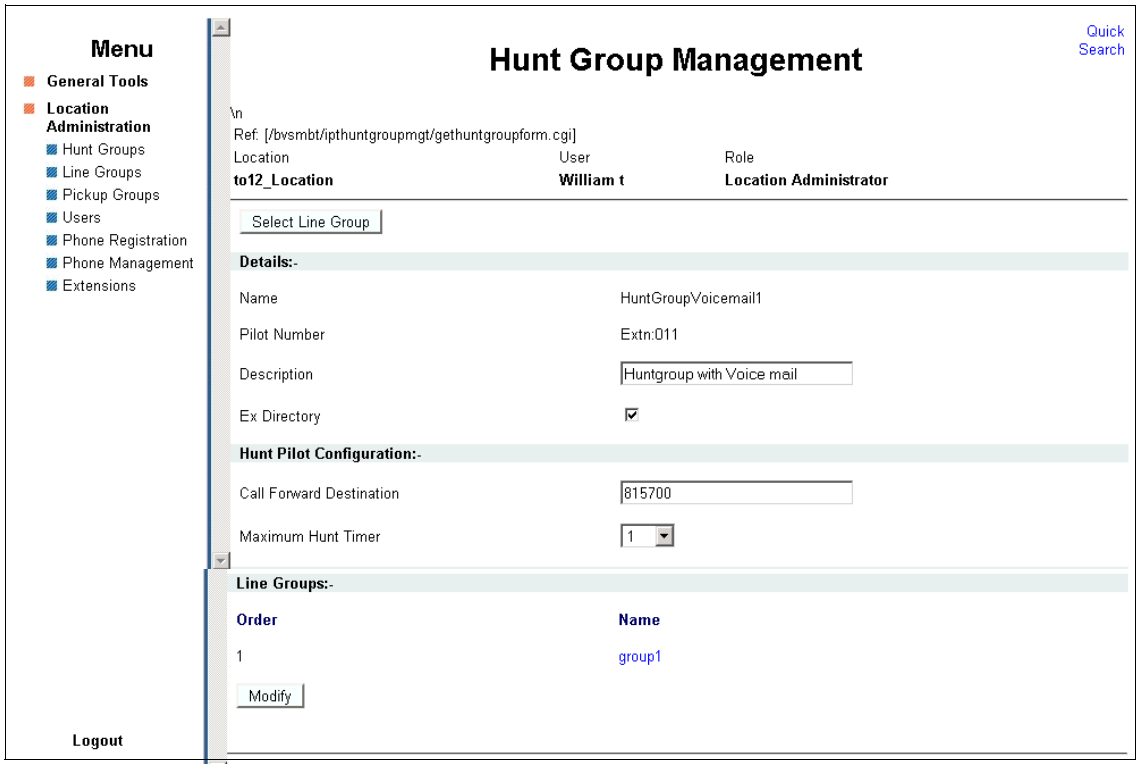


To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click the link for the hunt group you want to manage in the Name column.

The page shown in Figure A-5 appears.

Figure A-5 Hunt Group Management



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-8)
- 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.

The page shown in Figure A-6 appears.

Figure A-6 Select Line 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.

Note Before you can add a line group, you must first create the line group, as described in the "Line Groups" section on page A-10.

Step 6 Click **Submit**.

Step 7 Click **Return to Hunt Groups**.

Line Groups

A line group is a set of lines 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.

Creating a Line Group

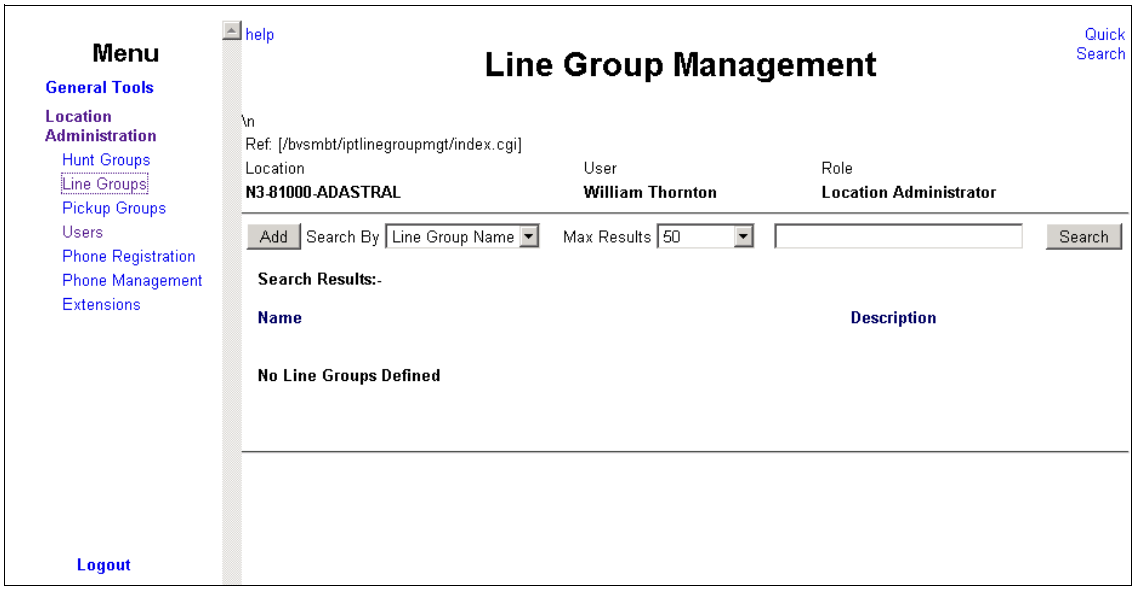
To create a line group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Line Groups**.

The Line Group Management page appears (see Figure A-7):

Figure A-7 Line Group Management

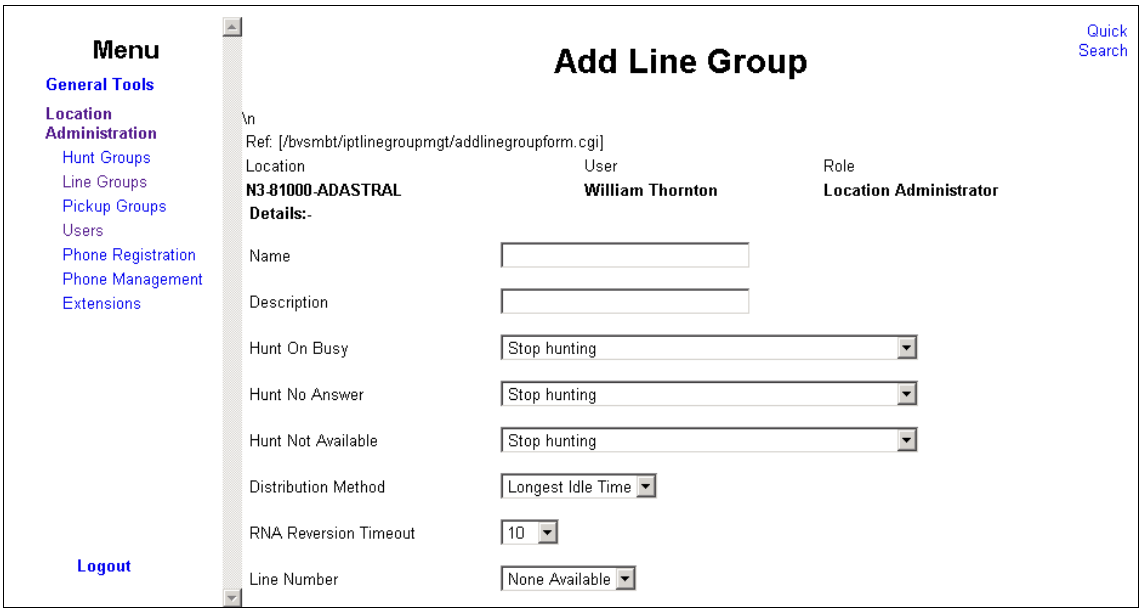


To search for a line group, select Line Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add** on the Line Group Management Page

The Add Line Group page appears (see Figure A-8):

Figure A-8 Add Line Groups



Step 3 Enter a unique name for the line group.

Step 4 (Optional) Enter a description for the line group.

Step 5 Select a behavior for the hunt group from each pull-down selection list for the following circumstances:

- Hunt on Busy—Perform the selected behavior when the line is busy.
- Hunt No Answer—Perform the selected behavior when the line is not answered.
- Hunt Not Available—Perform the selected behavior when the line is not answered

The behavior can be one of the following:

- Stop hunting
- Try next member, then, try next group in Hunt List
- Skip remaining members, and go directly to next group
- Try next member but do not go to next group

Step 6 Select the distribution method from the pull-down selection list:

- Longest Idle time
- Circular
- Top Down
- Broadcast

This determines the order in which the numbers within the number list are called when a call is directed to the pilot number assigned to the hunt group that uses this line group.

Step 7 Select the length of the Ring No Answer (RNA) Reversion Timeout from the pull-down selection list.

This value should be configured short enough to allow each line to be called before the Maximum Hunt Timer, specified in any associated Hunt Group, expires.

The maximum length of time that can be set for this timer is 180 seconds (3 minutes).

Step 8 Select the line number from the pull-down selection list.

Step 9 Click **Add**.

Adding a Line to a Line Group

A line group contains a series of lines that are used by a hunt group for directing an incoming call. To add a number to a line group, complete the following steps:

Procedure

Step 1 Select the name of the line list on the Line Group Management page.

The Manage Line Group page appears.

Step 2 Click **Add Line** on the Manage Line Group page.

The Add Line page appears:

Step 3 Select the required number from the drop-down selection list.

Step 4 Click **Add**.

Step 5 Repeat steps 2 through 4 for each number you need to add to the line group.

Step 6 To reorder the numbers in a line group, click **Re-Order** on the Manage Line Group page.

Step 7 Select and highlight the line to be re-ordered

Step 8 Click **Move Up** or **Move Down** to reposition the line.

Step 9 When all the lines are correctly positioned, click Update.

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 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.

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

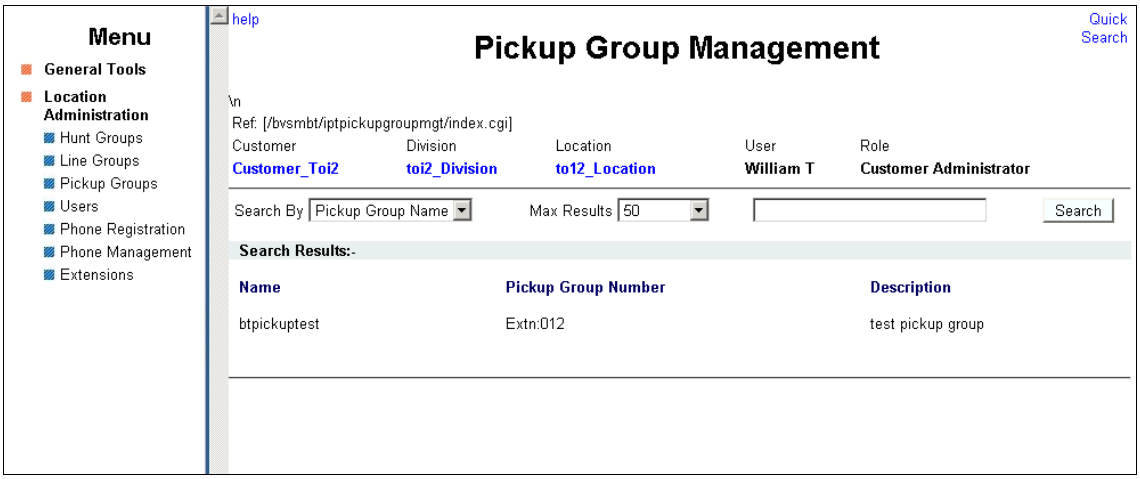
To add numbers to an existing pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

The Pickup Group Management page appears (see Figure A-9).

Figure A-9 Pickup Group Management

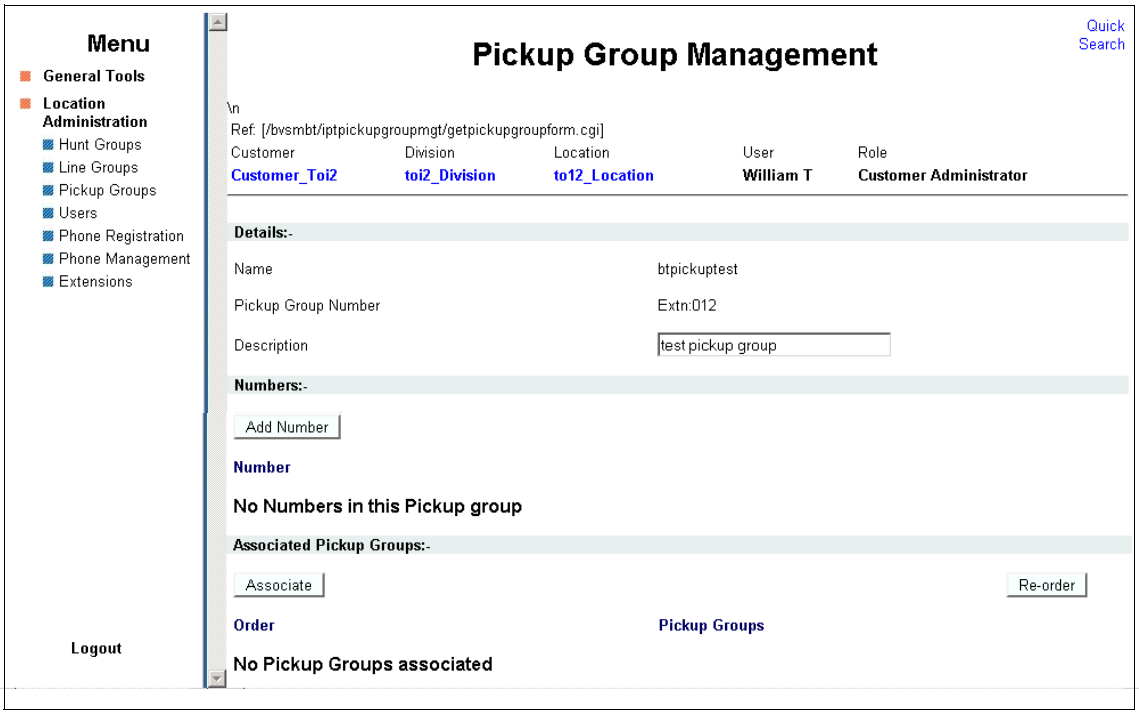


To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Select the name of the pickup group on the Pickup Group Management page.

The page shown in Figure A-10 appears.

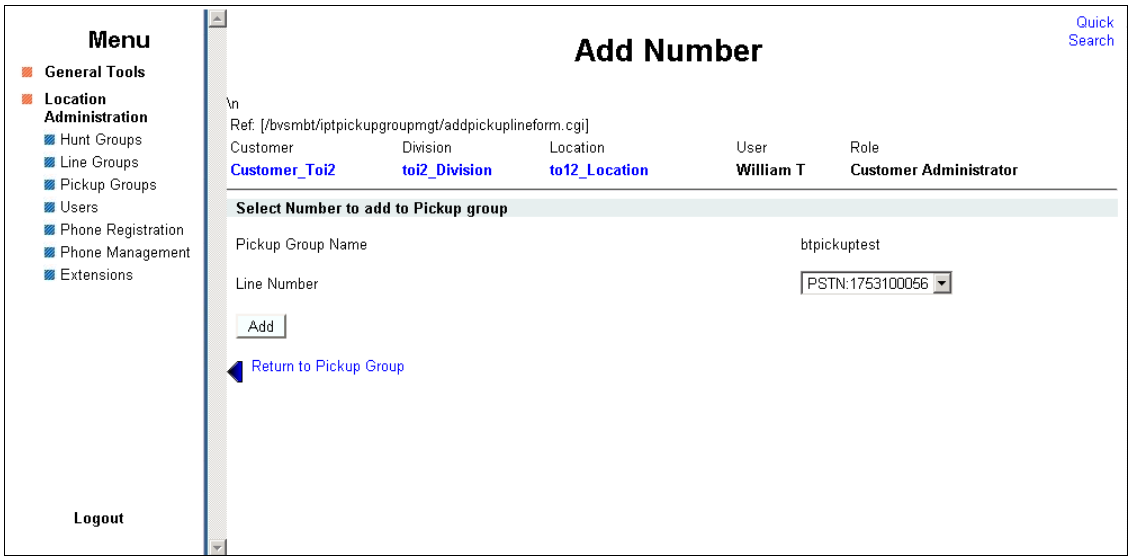
Figure A-10 Pickup Group Management



Step 3 Click **Add Number** on the Pickup Group Management page.

The Add Number page shown in Figure A-11 appears.

Figure A-11 Add Number



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 for 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**.

The Pickup Group Management page appears (see Figure A-9).

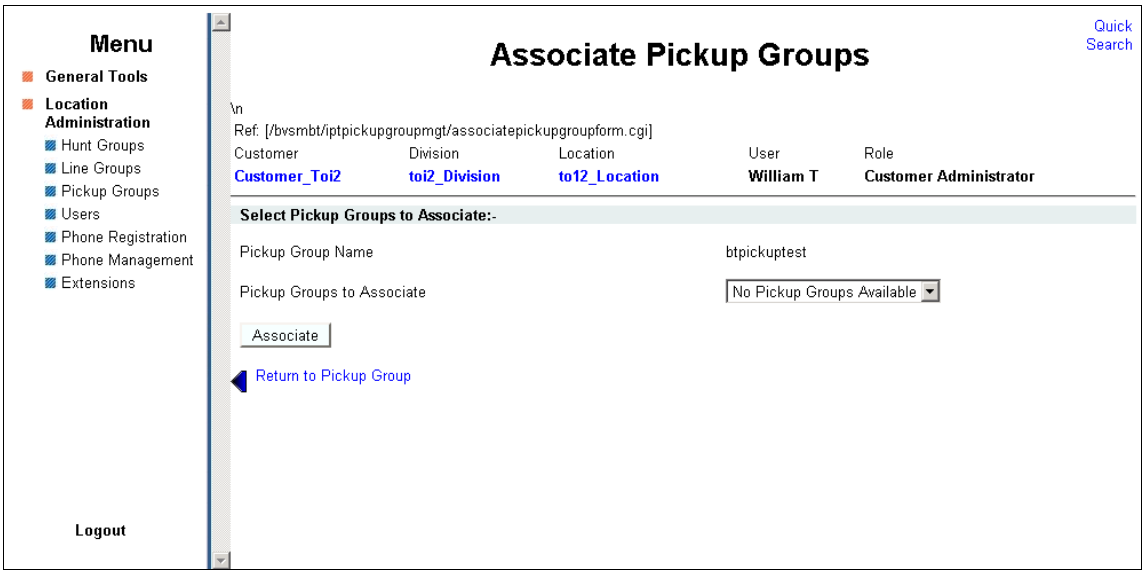
Step 2 Select the name of the pickup group on the Pickup Group Management page.

The page shown in Figure A-10 appears.

Step 3 Click **Associate**.

The page shown in Figure A-12 appears.

Figure A-12 Associate Pickup Groups



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

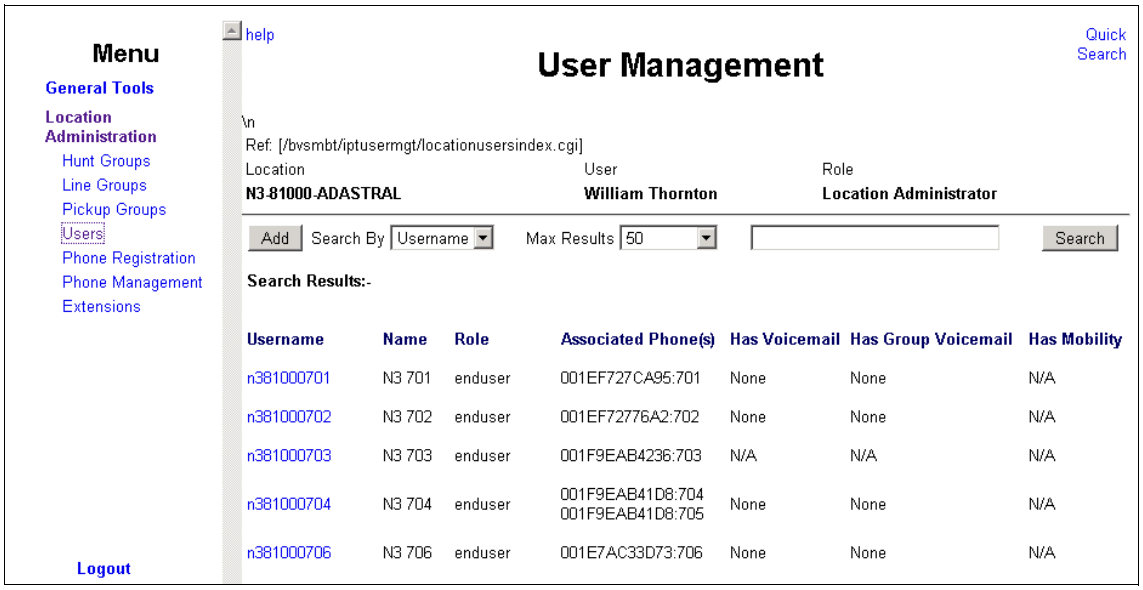
This section describes the following tasks that you can perform using the Users option on the Location Administration menu:

- Adding a User Account, page A-17
- Deleting a User Account, page A-24
- Managing Voice Mail Accounts, page A-20
- Managing Mobility Profiles, page A-21
- Associating and Unassociating a Phone with a User, page A-22

Managing User Accounts

The User Management page (Figure A-13) 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-13 User Management



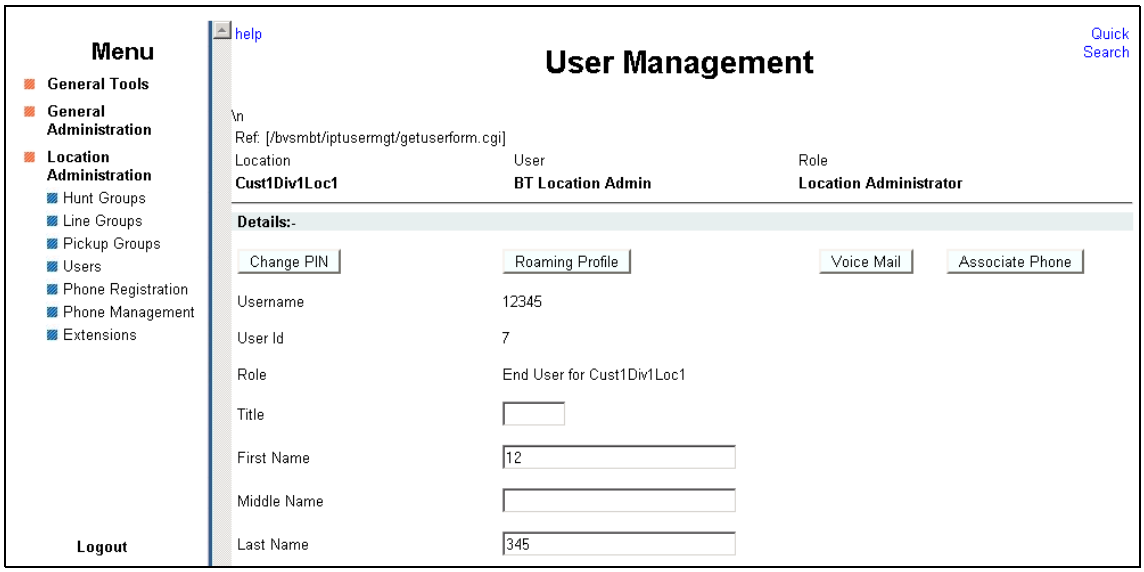
To search for a user account, select Username or Surname (last name) from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

Step 1 To manage an existing user account, click the blue entry in the Username column.

Note Links that you click to display another page are bright blue.

The User Account Management page appears (Figure A-14).

Figure A-14 User Account Management



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.

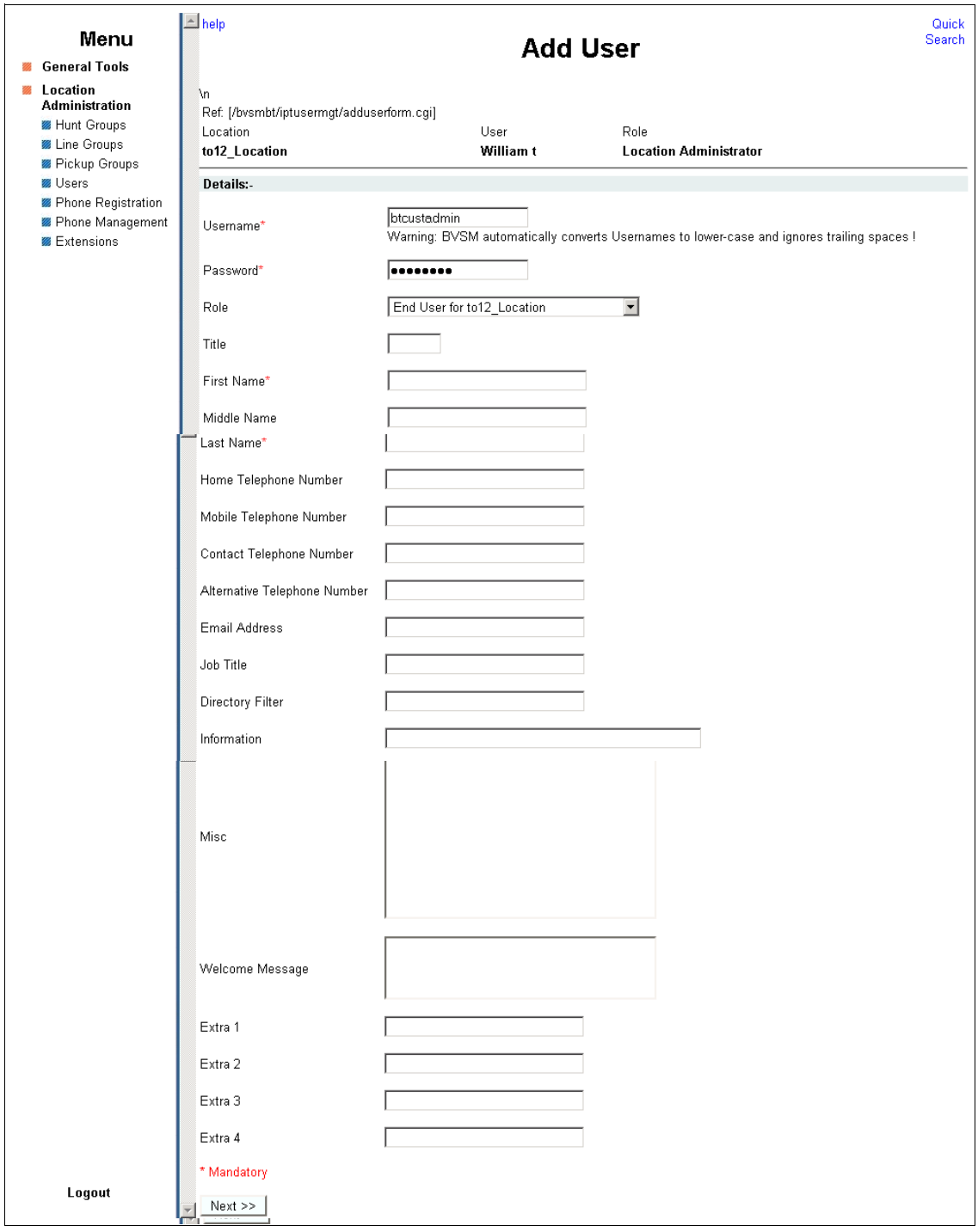
To add a new user account, complete the following steps:

Procedure

Step 1 On the User Management page (Figure A-13), click **Add**.

The page shown in Figure A-15 appears:

Figure A-15 Add User—Page 1



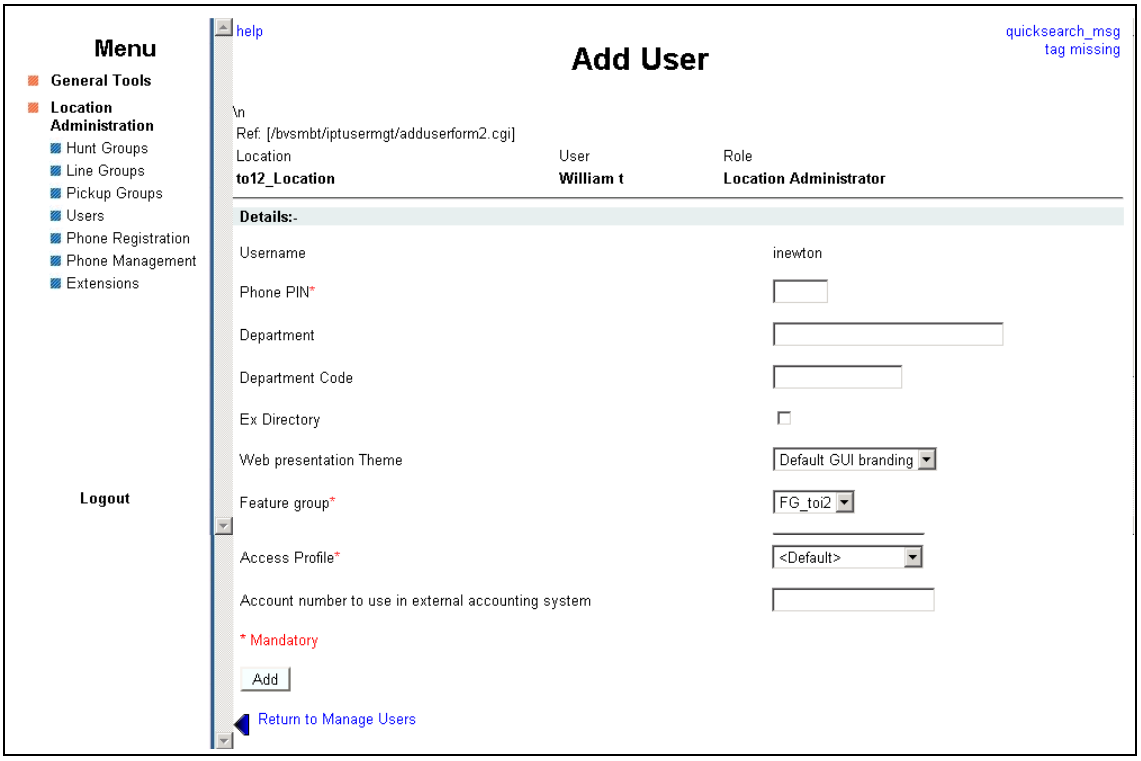
Step 2 Enter the details for the user account in the fields provided.

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**. The page shown in Figure A-16 appears:

Figure A-16 Add User—Page 2



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 (Optional) complete the other fields as required in your location.

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.

Select the BT Enduser Profile to provide standard permissions.

Step 7 Enter the account number to be used for accounting purposes.

Step 8 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

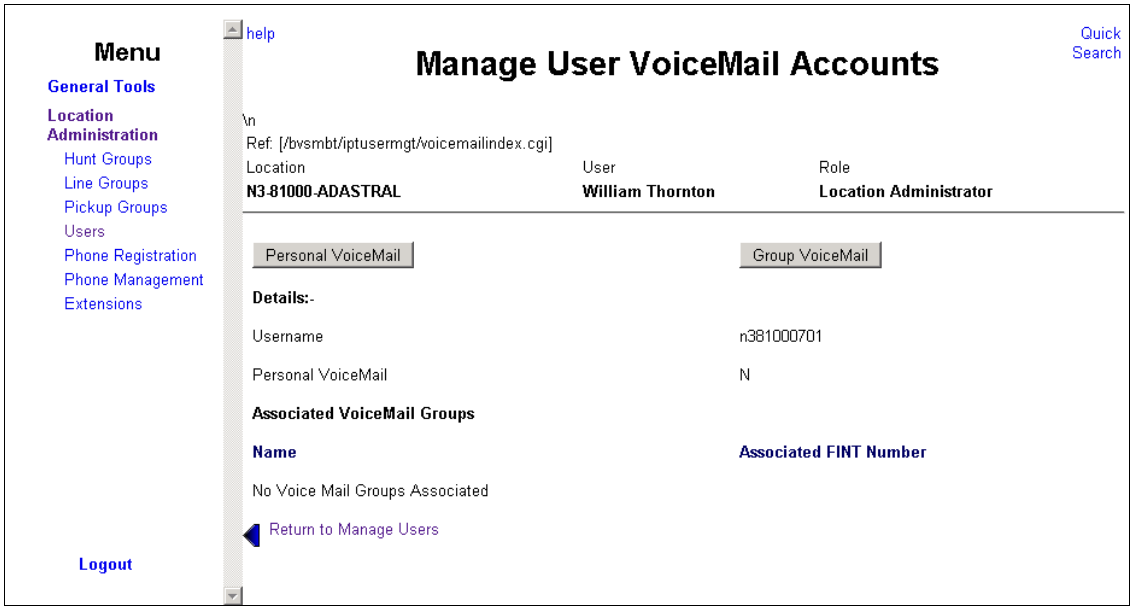
Step 1 On the User Management page (Figure A-13), click the blue entry in the Username column.

The User Account Management page appears (Figure A-15).

Step 2 On the User Account Management page, click **VoiceMail**.

The page shown in Figure A-17 appears:

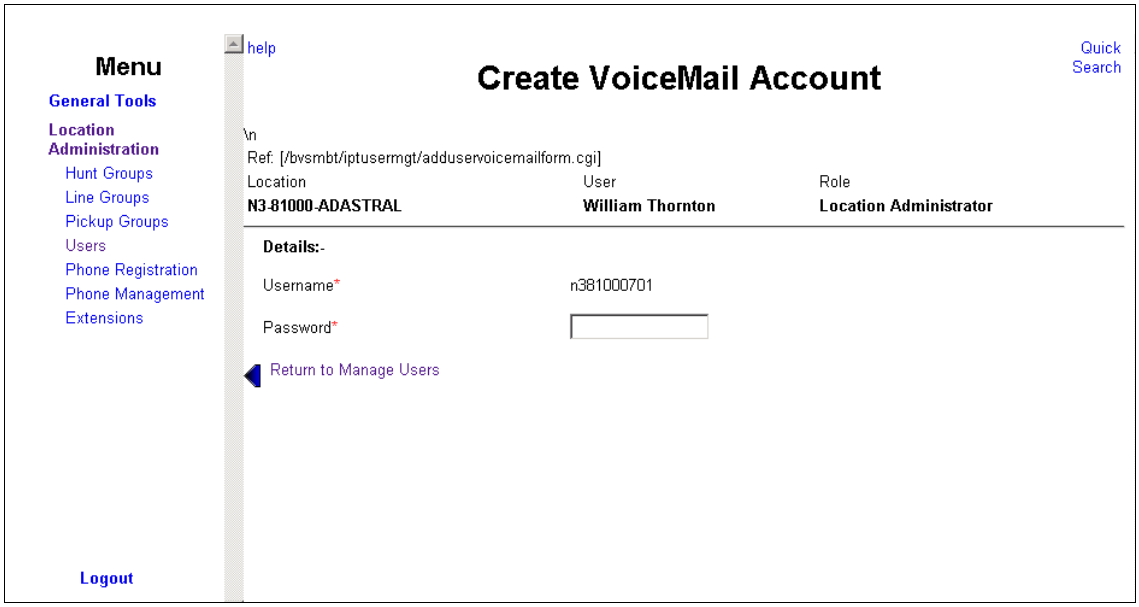
Figure A-17 Manage User VoiceMail Accounts



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.

The page shown in Figure A-18 appears:

Figure A-18 Create VoiceMail Account



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

Note For details about using each option on the Manage Mobility Profile page, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b)*.

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

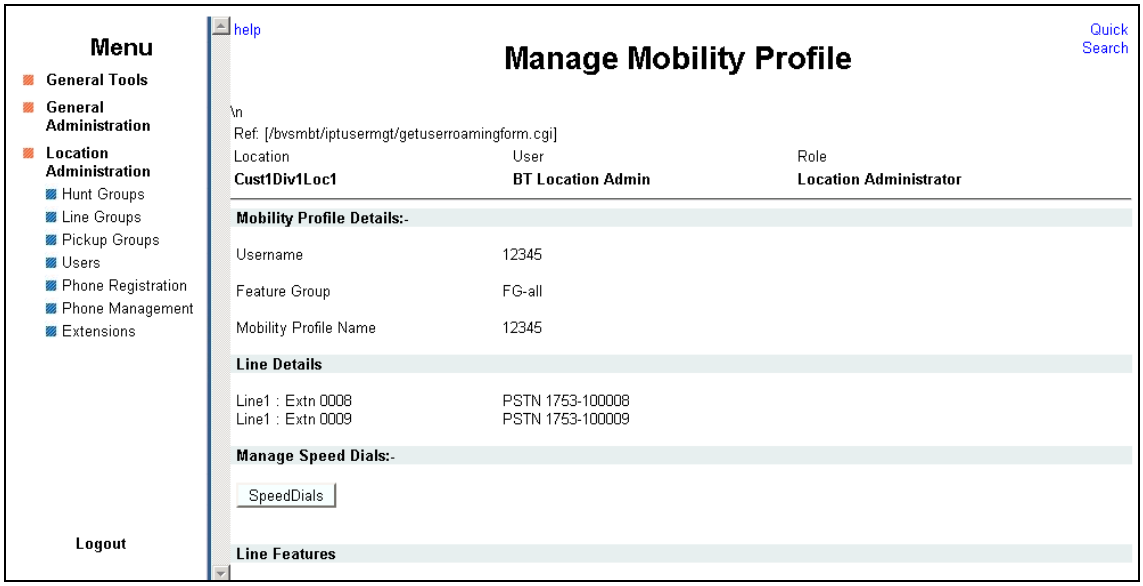
Step 1 On the User Management page (Figure A-13), click the blue entry in the Username column.

The User Account Management page appears (Figure A-15).

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 (Figure A-19).

Figure A-19 Add Mobility Profile



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 modify the mobility profile, make your changes Manage Mobility Profile page and click **Modify**.

The options available on the Manage Mobility Profile page are similar to those for the Phone Management page. For detailed information about these fields, refer to *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b)*.

Step 5 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 (Figure A-13), click the blue entry in the Username column.

The User Account Management page appears (Figure A-15).

Step 2 On the User Account Management page, click **Phone Associate**.

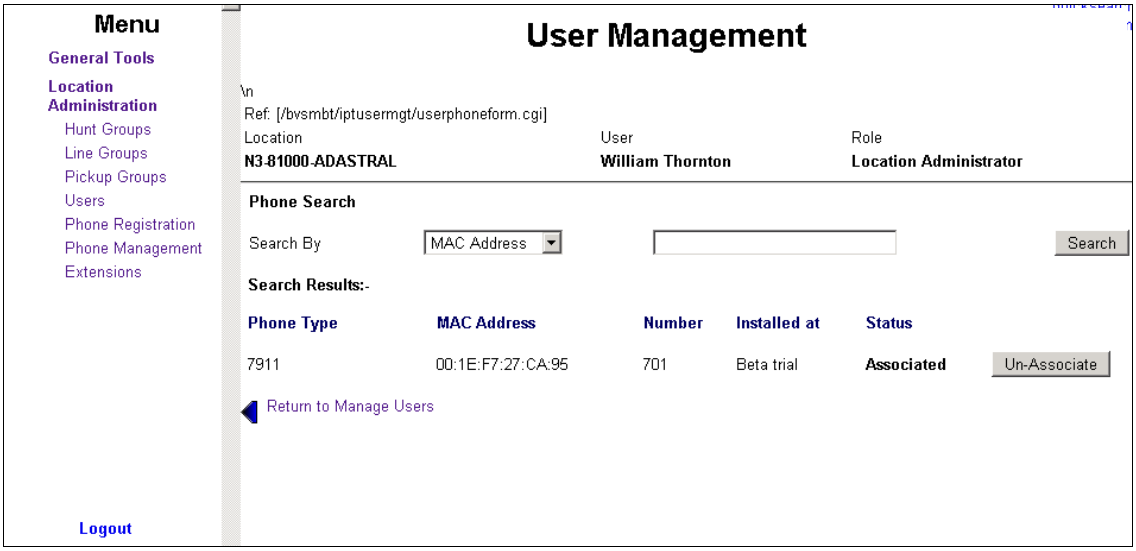
A list of available phones appears that are not already associated with another user account. Determine which phone has been registered to be associated with the User.

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 3 Click **Associate Phone**.

Step 4 To unassociate a phone, click **Un-Associate** on the User Management page shown in Figure A-20.

Figure A-20 User Management—Associating and Unassociating a Phone



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 (Figure A-13), click the blue entry in the Username column for the account you want to delete.

The User Account Management page appears (Figure A-15).

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 BVSM 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.

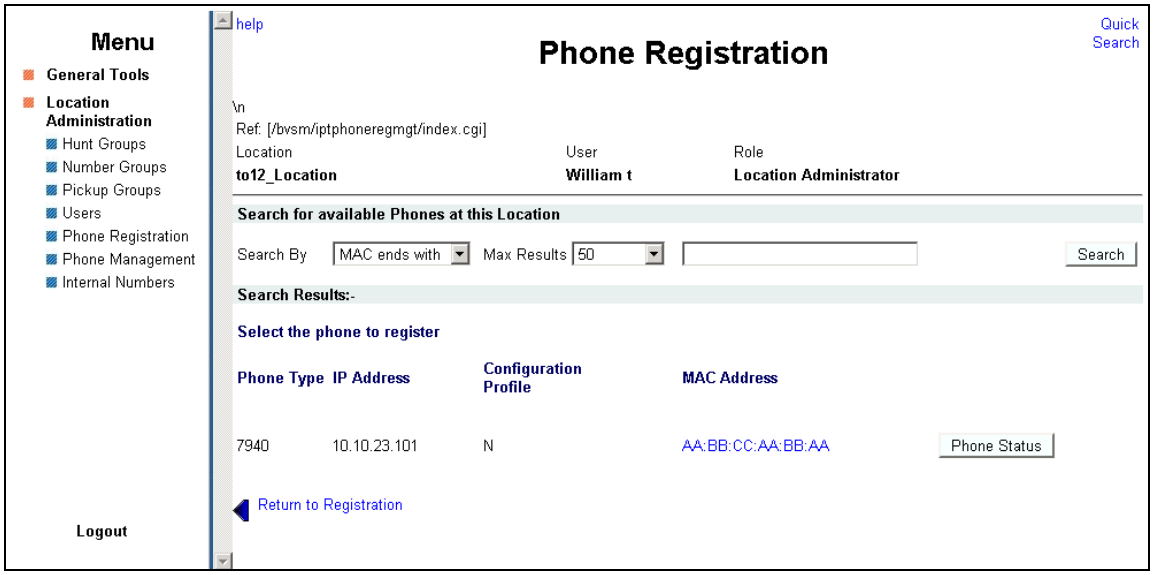
To register a phone, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration menu.

The Phone Registration page appears (Figure A-21).

Figure A-21 Phone Registration



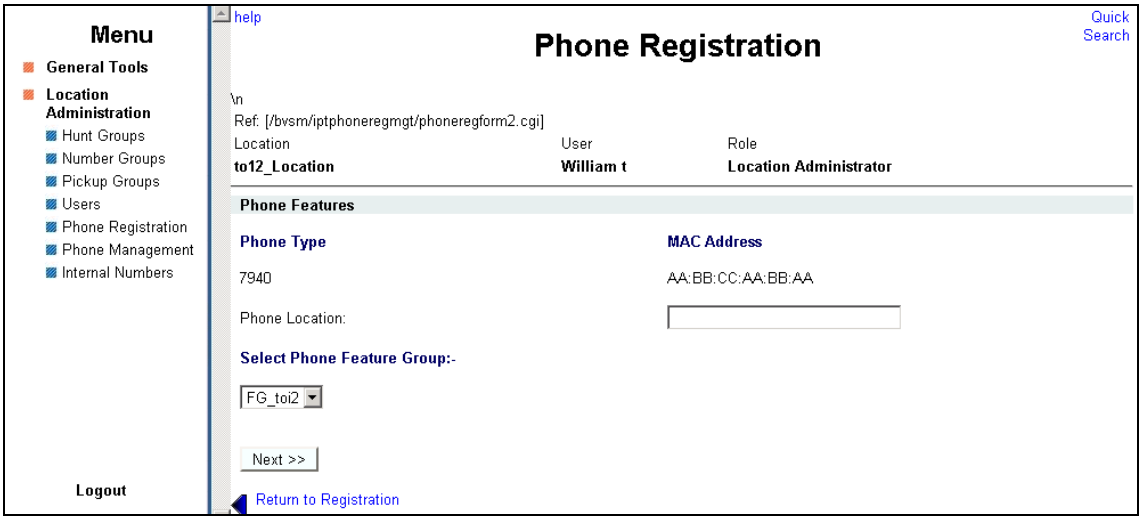
To search for a phone, select MAC ends with or Phone Type from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is *not* case-sensitive.

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.

The page shown in Figure A-21 appears.

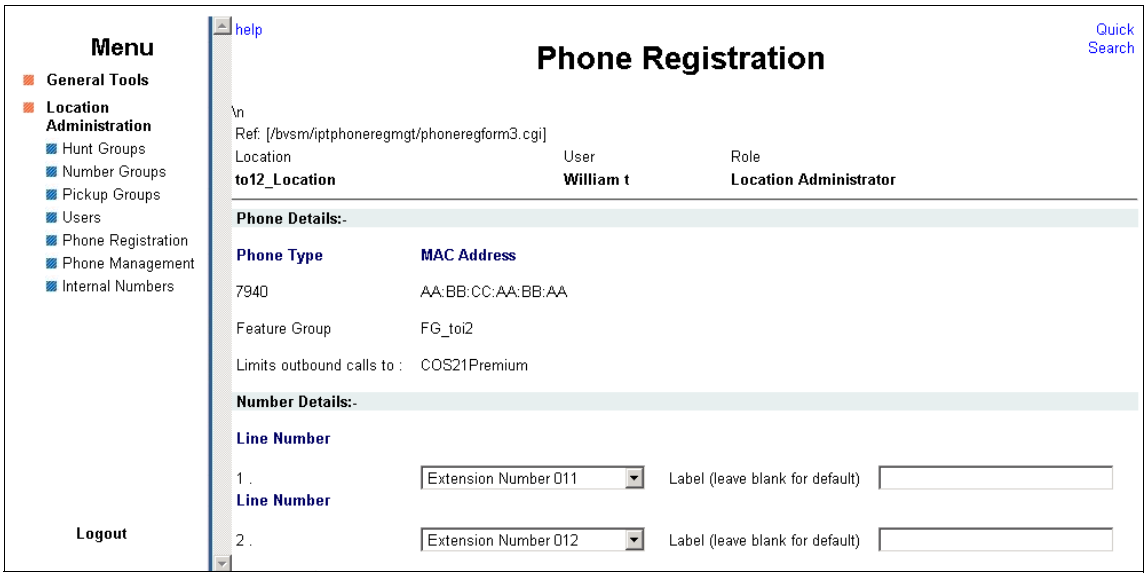
Figure A-22 Phone Registration



Step 3 Select the feature group to use with the phone from the pull-down selection list.

The page shown in Figure A-21 appears.

Figure A-23 Phone Registration



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

For details about using each option on the Phone Management page, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b).*

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.

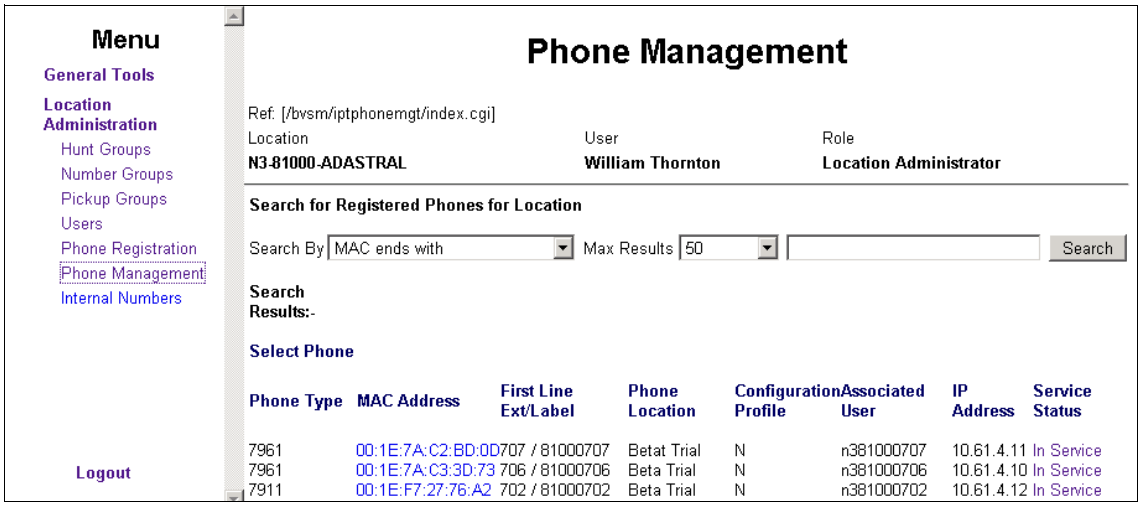
To manage any phone at your location, complete the following steps:

Procedure

Step 1 Select the **Phone Management** option from the Location Administration menu.

The Phone Management page appears (Figure A-21).

Figure A-24 Phone Management



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 shown in Figure A-21 appears.

Figure A-25 Phone Management

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.

For details about using each option on the Phone Management page, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b)*.

Extensions

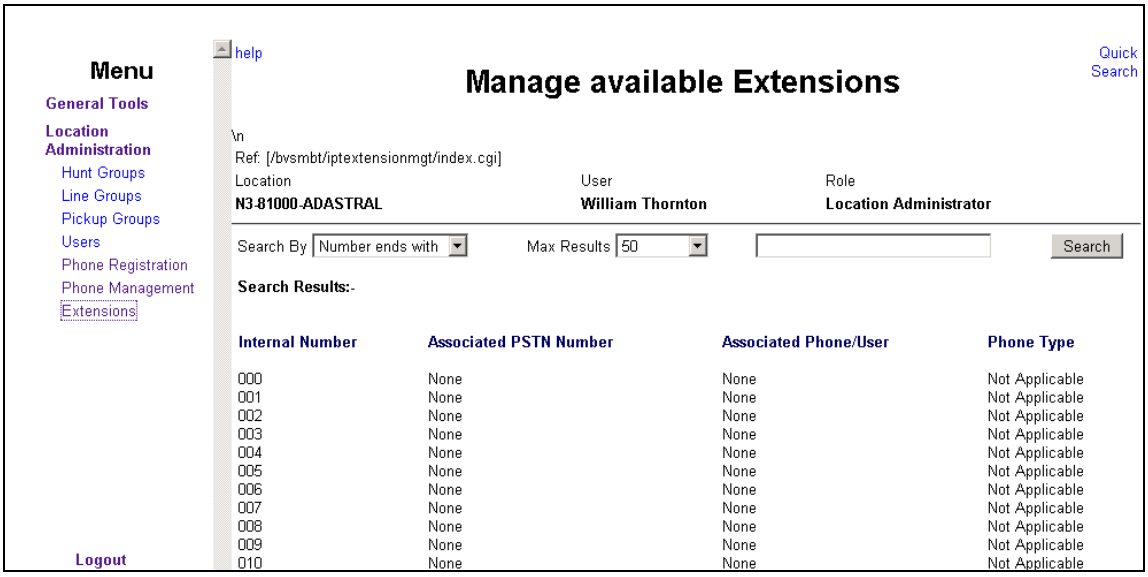
To manage the extensions at your location, complete the following steps:

Procedure

Step 1 Click the **Extensions** option on the Location Administration menu.

The Manage available Extensions page shown in Figure A-26 appears.

Figure A-26 Manage Available Extensions



The Manage available Extensions 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

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:

- Resources/Phone Inventory, page B-7
- General Tools, page B-10
- General Administration, page B-13
- Location Administration, page B-22

Note For additional information about using the options on the Location Administration menu, refer to Appendix A, Hosted UCS Location Administration. For information about using the options on the Self Care menu, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b)*.

Overview

This section includes the following topics:

- User Interface Guidelines, page B-1
- Quick Search, page B-2
- Managing Phones, page B-4
- Managing Internal and External Numbers, page B-6
- Managing Services, page B-6

User Interface Guidelines

Note the following conventions used in Hosted UCS menus and associated administration pages:

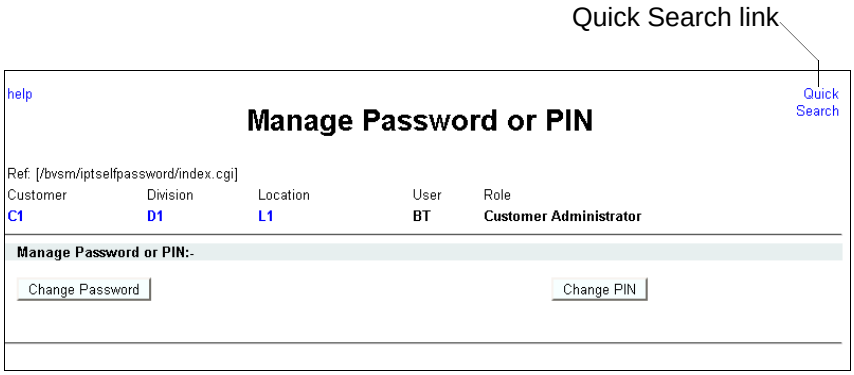
- Links to other pages are bright blue.

- 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

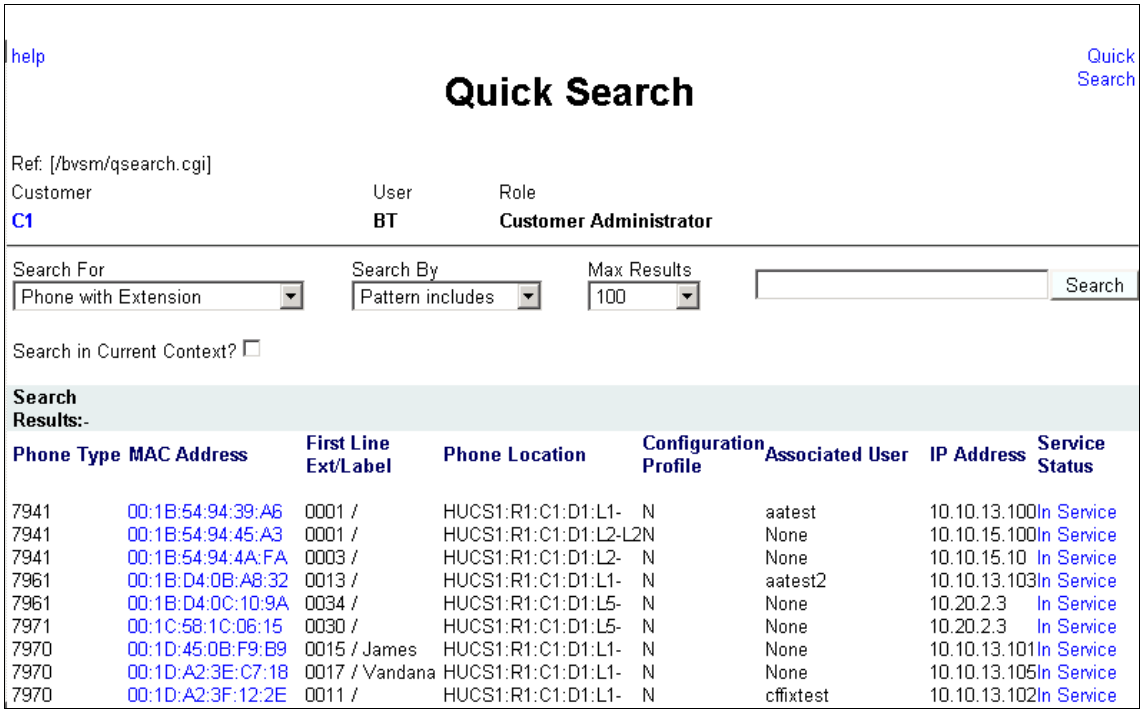
As shown in Figure B-1, each page of the BVSM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries 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 B-1 Quick Search Link



When you click the Quick Search link, the system displays the page shown in Figure B-2

Figure B-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 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.

Table B-1 Search Types

Search Type	Description
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.

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-4
- Manually Adding Phones, page B-5
- Removing Phones, page B-5

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 BVSM 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 BVSM 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 BVSM.

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- 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.

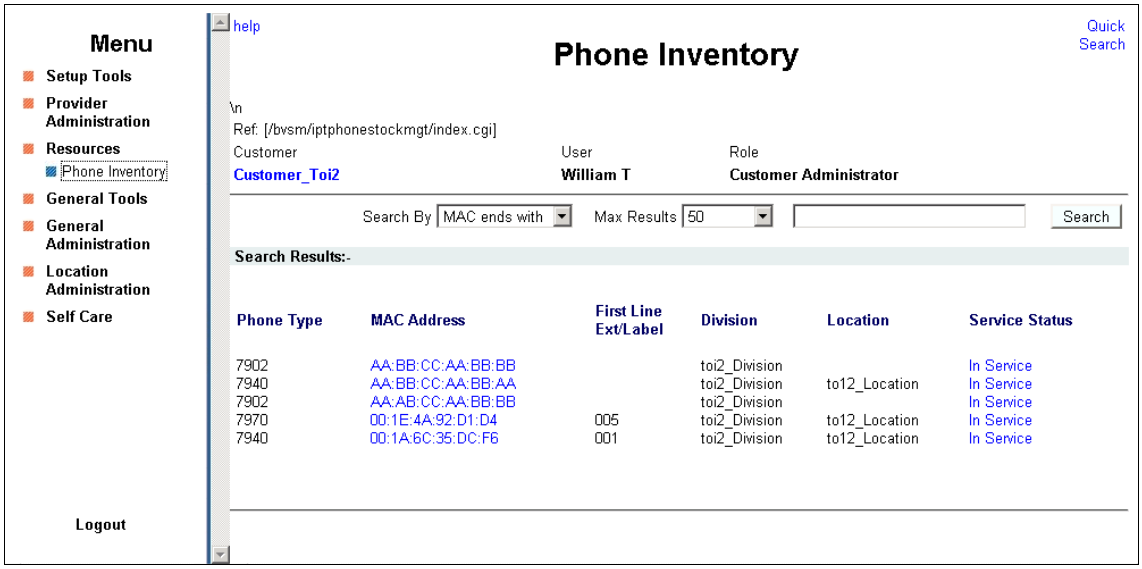
To view the phone inventory or move a phone between locations, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the Resources Menu.

The screen shown in Figure B-3 appears.

Figure B-3 Phone Inventory



This page provides a list of the phones on the system with their location and status. To search for a phone, select one of the following options from the Search by pull-down selection list:

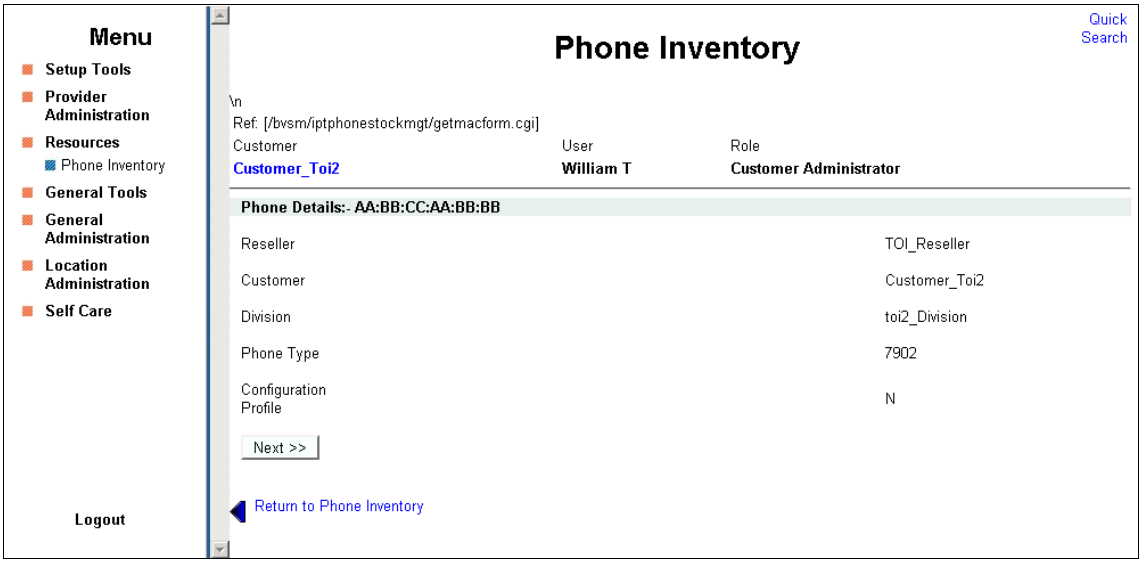
- MAC starts with
- MAC ends with
- Search by phone location
- Extension Number Ends with
- Extension Number Starts with
- Full Internal Number

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.

The screen shown in Figure B-4 appears.

Figure B-4 Allocate/Move Phone—Page 1



This page lists information about the selected phone and lets you move it to a different location.

Step 3 Click **Next**.

The screen shown in Figure B-5 appears.

Figure B-5 Allocate/Move Phone—Page 2

Step 4 Select the location to which you want to move the phone from the pull-down selection list.

Step 5 Click **Next**.

The screen shown in Figure B-6 appears.

Figure B-6 Allocate/Move Phone—Page 3

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.

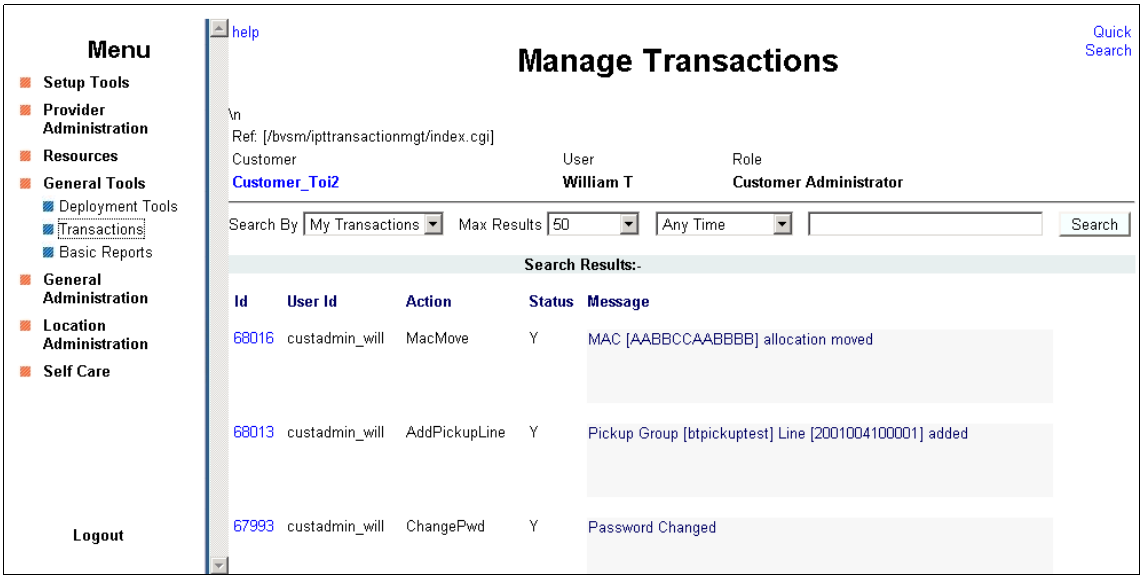
This section describes the following options on the General Tools menu.

- Transactions, page B-10
- Basic Reports, page B-11

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-7 appears.

Figure B-7 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)

Basic Reports

The following is a list of reports that are currently provided with BVSM:

- Directory List (under Self Care menu)
  - First Name
  - Second Name
  - Location
  - Extension Number
  - PSTN Number
- User List (under Location Administration)
  - User ID
  - User Name
  - Role

    - Provider, Reseller, Customer, Division, Locations
- Phone Inventory List (under Location Administration menu)
    - Phone Type
    - MAC Address
    - Reseller, Customer, Division, Locations
    - Registration status
    - IP Address
- Phone Management (under Location Administration)
    - Phone Type
    - MAC Address
    - 1st Line Number
    - Phone Location
    - Associated User
    - IP Address
- Internal Number Inventory (under Location Administration)
    - Internal Number
    - Associated E164 Number
    - Associated Phone/User
    - Switchboard Pilot
    - Phone Type

When you click the **Basic Reports** option, the screen shown in Figure B-8 appears.

Figure B-8 Reports

This page displays a list of the reports available.

Click the blue link in the Select Report Views to view a specific report.

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 option on the General Administration menu.

- Locations, page B-13

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.

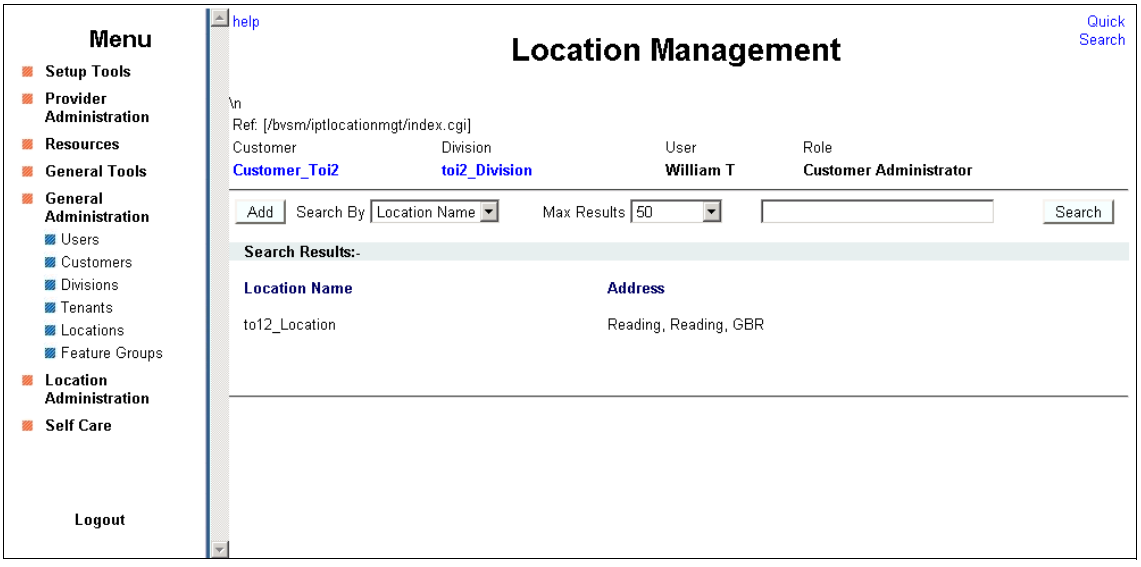
To add a new location, complete the following steps:

Procedure

Step 1 Select **Location** from the Location Administration menu.

The screen shown in Figure B-9 appears.

Figure B-9 Location Management



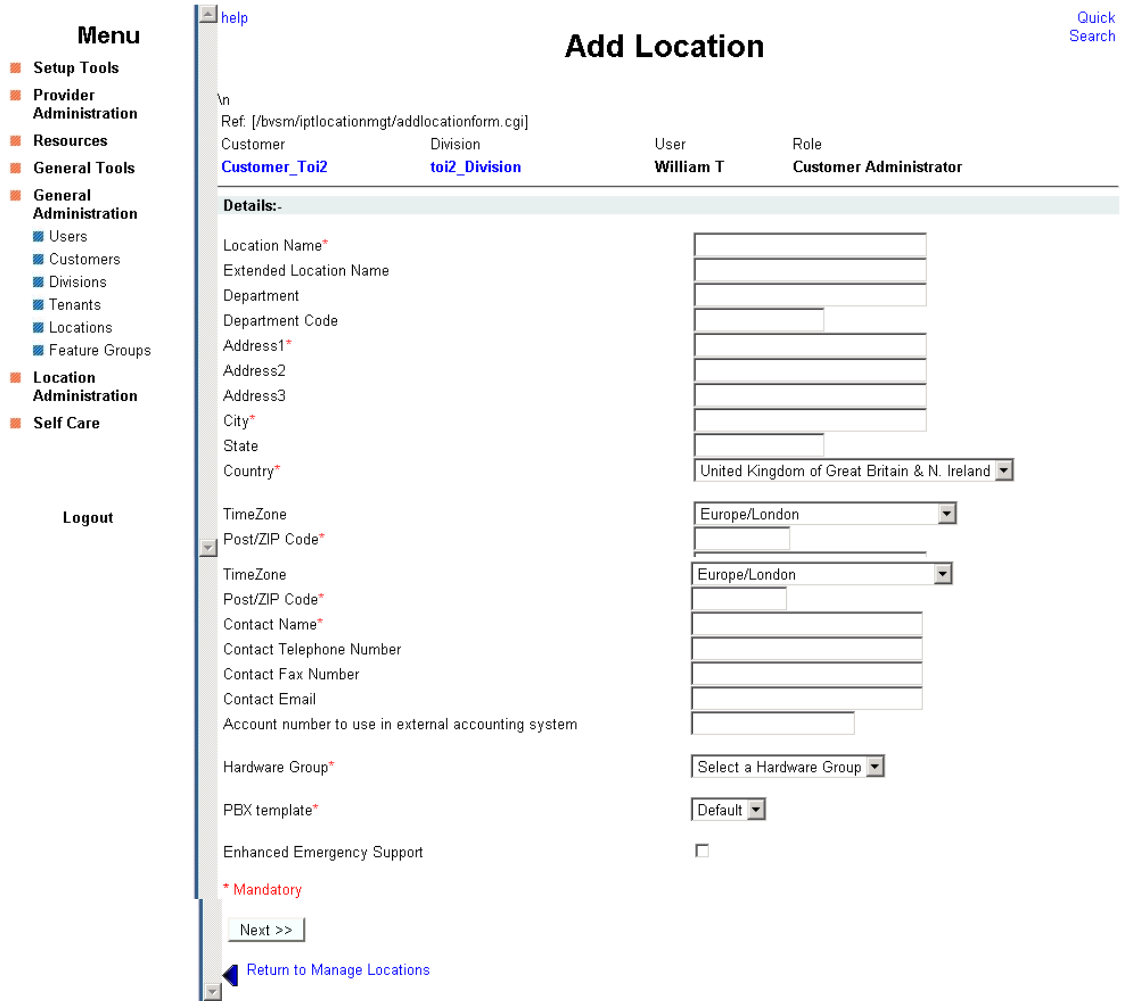
This page displays a list of the locations in the Hosted UCS system. You can use this page to search for locations in the database, to manage a specific location, or add a location.

Step 2 To manage an existing location, click the blue link in the Name column.

Step 3 To add a location, click **Add**.

The screen shown in Figure B-10 appears.

Figure B-10 Add Location



Step 4 Enter the details required for the current location.

The mandatory fields are indicated by a red asterisk.

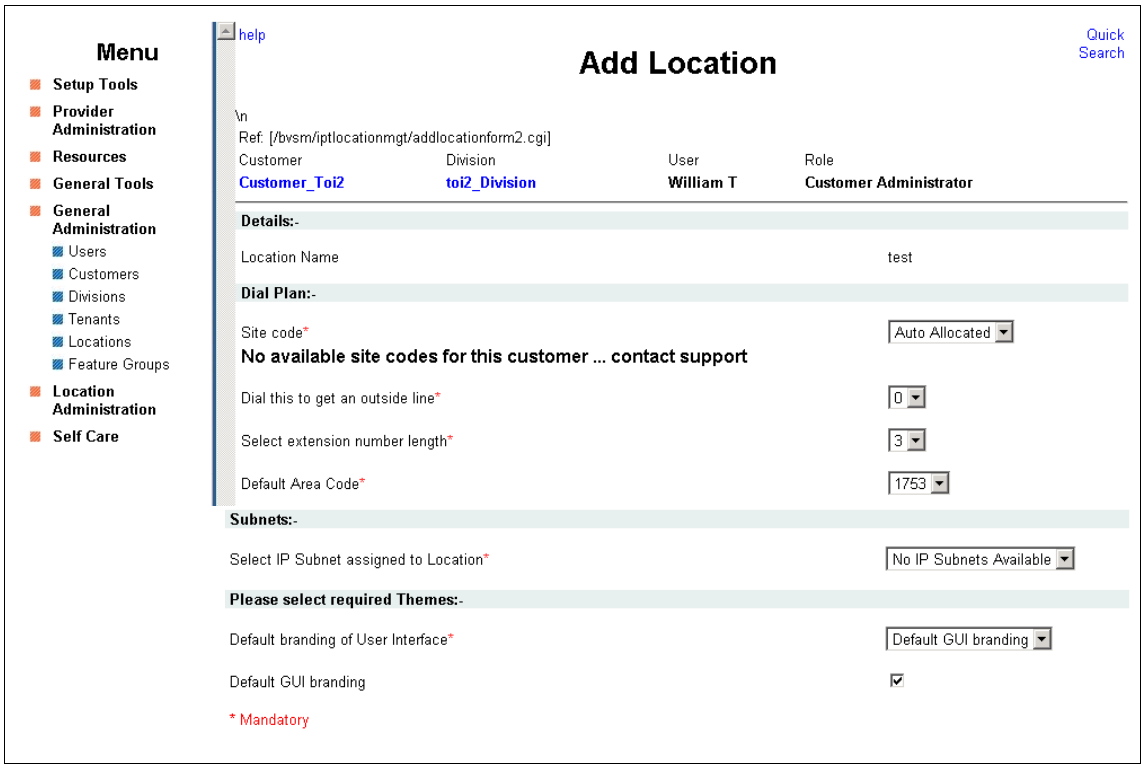
Step 5 Select Hardware Group from the drop-down menu.

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**.

The screen shown in Figure B-11 appears.

Figure B-11 Add Location—Page 2



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.

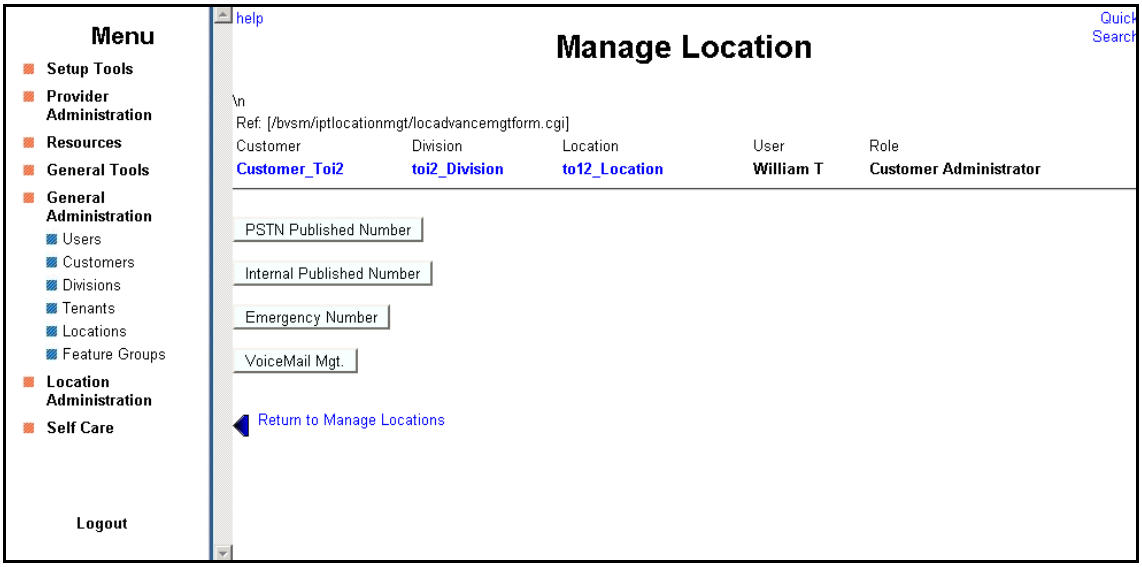
Managing Location Resources

The screen shown in Figure B-12 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.

Figure B-12 Manage Location



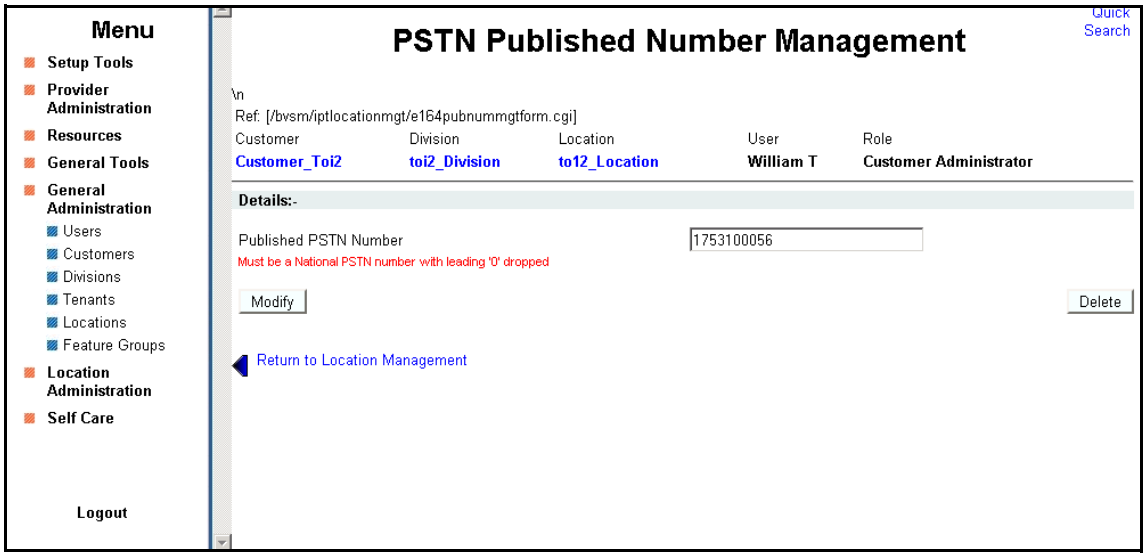
PSTN Published Number

To manage the PSTN numbers for the current location, complete the following steps:

Procedure

Step 1 Click **PSTN Published Number**.

Figure B-13 PSTN Published Number Management



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

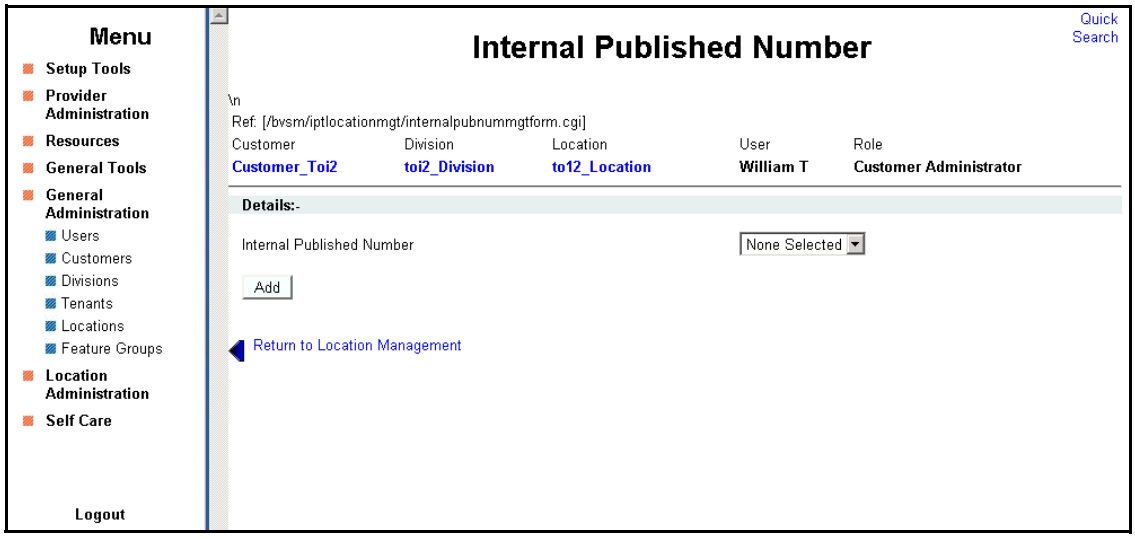
To manage the internal published numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Internal Published Number**.

The screen shown in Figure B-14 appears.

Figure B-14 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

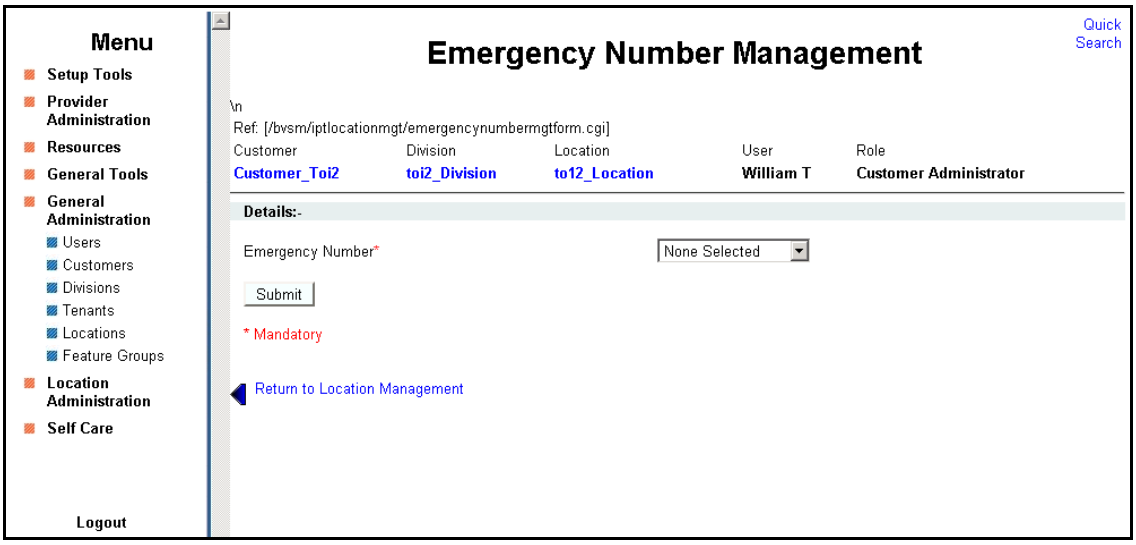
To manage the emergency numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Emergency Number**.

The screen shown in Figure B-15 appears.

Figure B-15 Emergency Number Management



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.

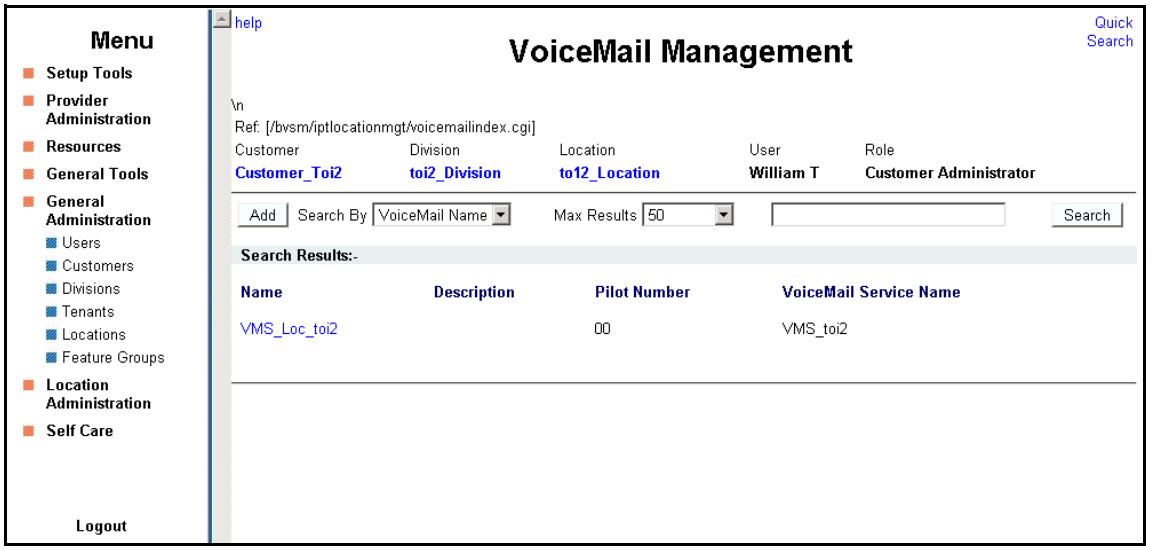
To manage voicemail services, complete the following steps:

Procedure

Step 1 Click **VoiceMail Mgt**. on the Manage Location page.

The screen shown in Figure B-16 appears.

Figure B-16 VoiceMail Management



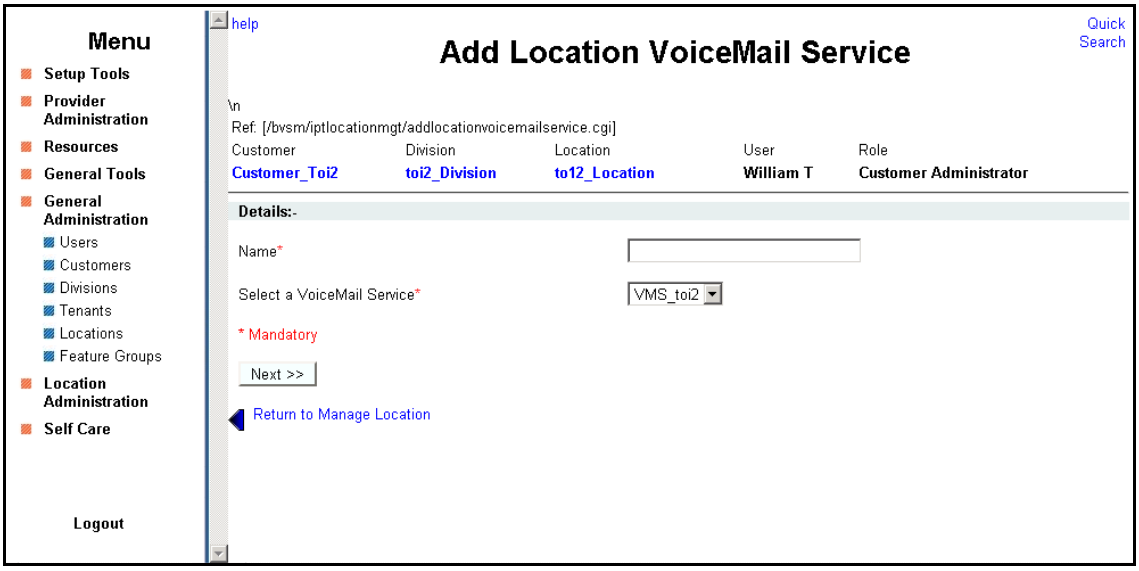
This page displays a list of the voicemail services in the current location. You can use this page to search for voicemail services in the database, to manage a specific voicemail service, or add a voicemail service.

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**.

The screen shown in Figure B-17 appears.

Figure B-17 Add Location VoiceMail Service



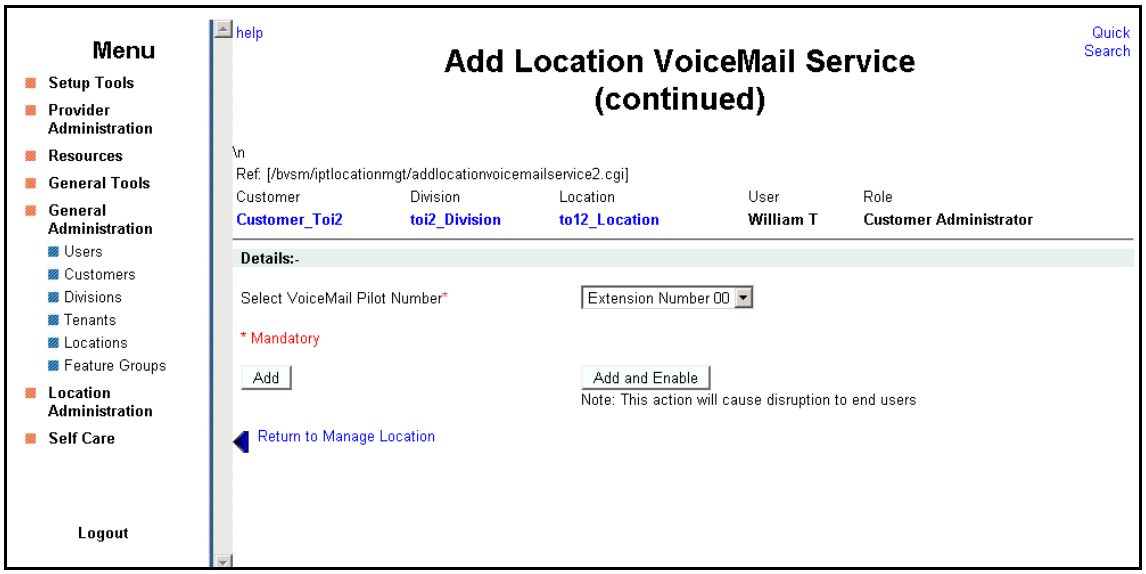
Step 4 Enter the voicemail service name.

Step 5 Select the voicemail resource from the pull-down selection list.

Step 6 Click **Next**.

The screen shown in Figure B-18 appears.

Figure B-18 Add Location VoiceMail Service (continued)



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.

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.

- Hunt Groups, page B-23
- Number Groups, page B-25
- Voicemail Groups, page B-25
- Pickup Groups, page B-27
- Users, page B-28
- Phone Registration, page B-31
- Phone Management, page B-32

- Internal Numbers, page B-32

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-25. 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, "Location Administration."

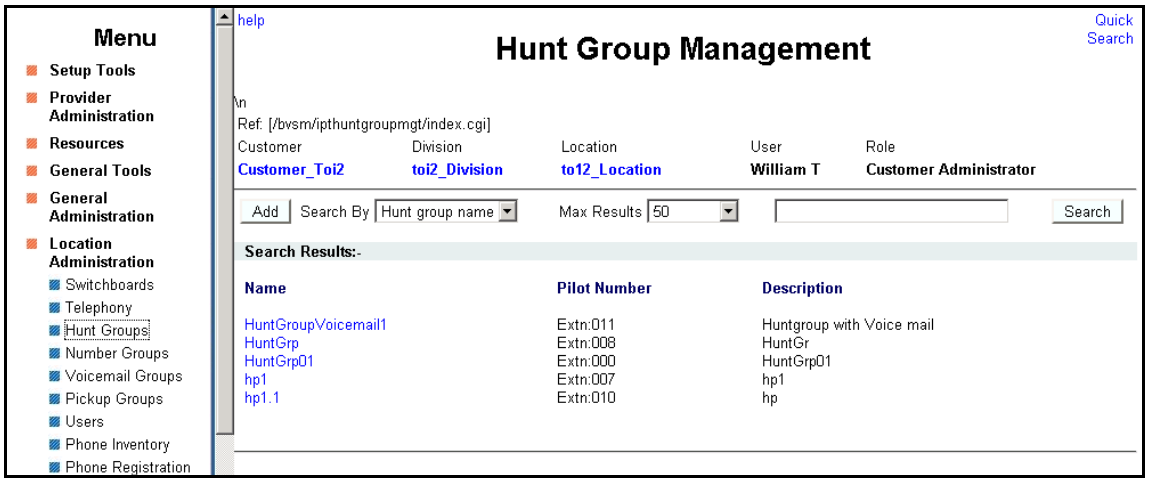
To create a hunt group, complete the following steps:

Procedure

Step 1 Select **Hunt Groups** on the Location Administration menu.

The Hunt Group Management page appears (see Figure B-19).

Figure B-19 Hunt Group Management

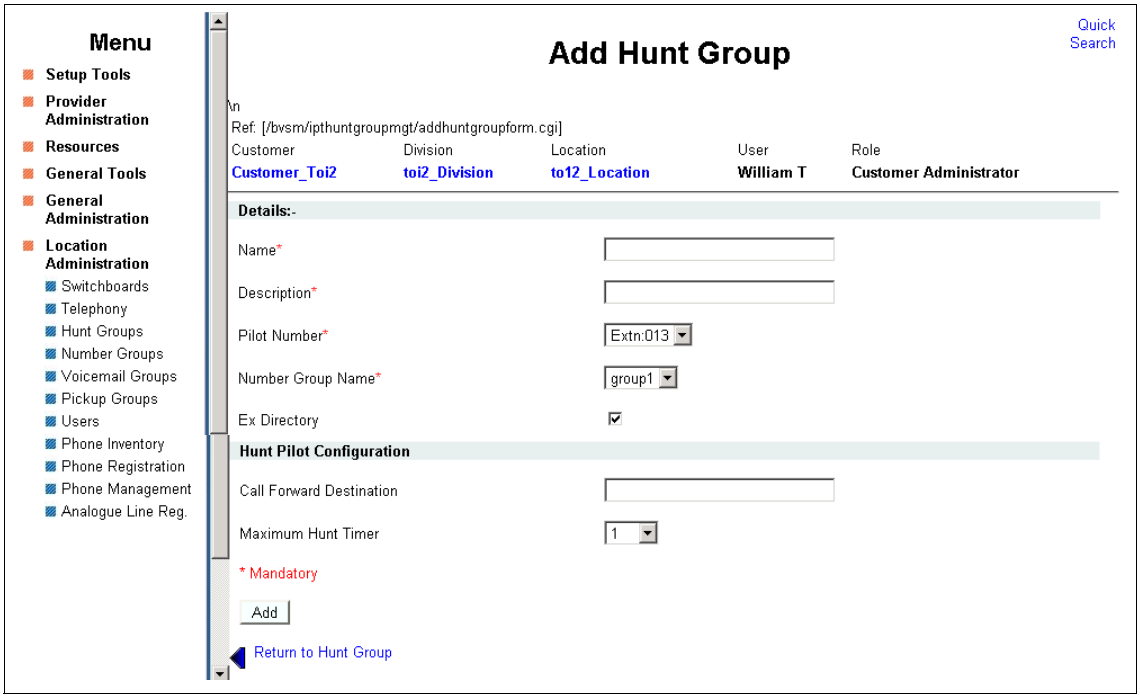


To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add**.

The page shown in Figure B-20 appears.

Figure B-20 Add Hunt Group



Step 3 Enter a unique name for the hunt group.

Step 4 (Optional) Enter a description for the hunt group.

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, “Location Administration.”

Note Number groups in the location administrator level are called line groups.

Voicemail Groups

Once a voicemail resource has been created for a customer, it can be allocated to a location by creating a voicemail service within the location. Once a voicemail service exists within a location, then user accounts can be created using an associated phone or Mobility profile). Once the user account is created, the user can manage their own voicemail account through the Self Service menu.

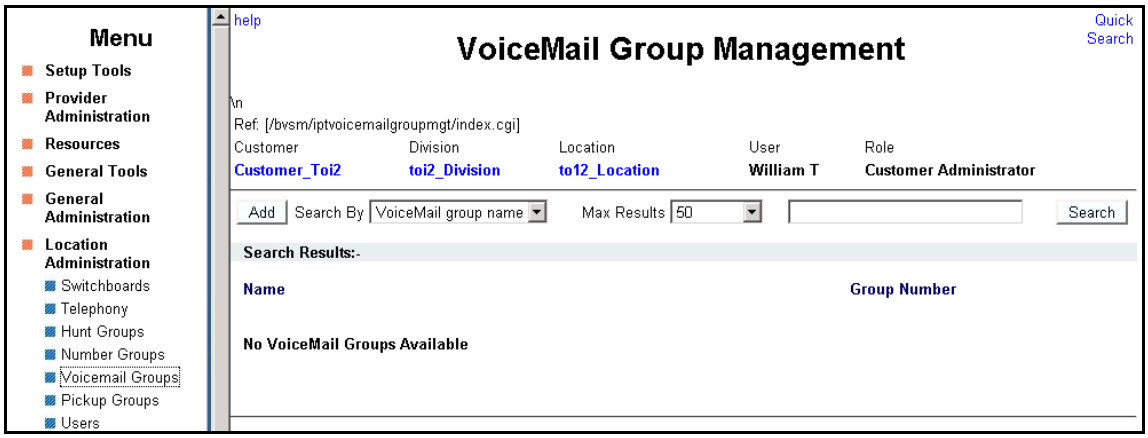
Use the **VoiceMail Groups** option on the Location Administration menu to manage existing voicemail group or to create a new voicemail group. To manage voicemail groups, complete the following steps:

Procedure

Step 1 Select **VoiceMail Groups** on the Location Administration Menu.

The screen shown in Figure B-21 appears.

Figure B-21 VoiceMail Group Management



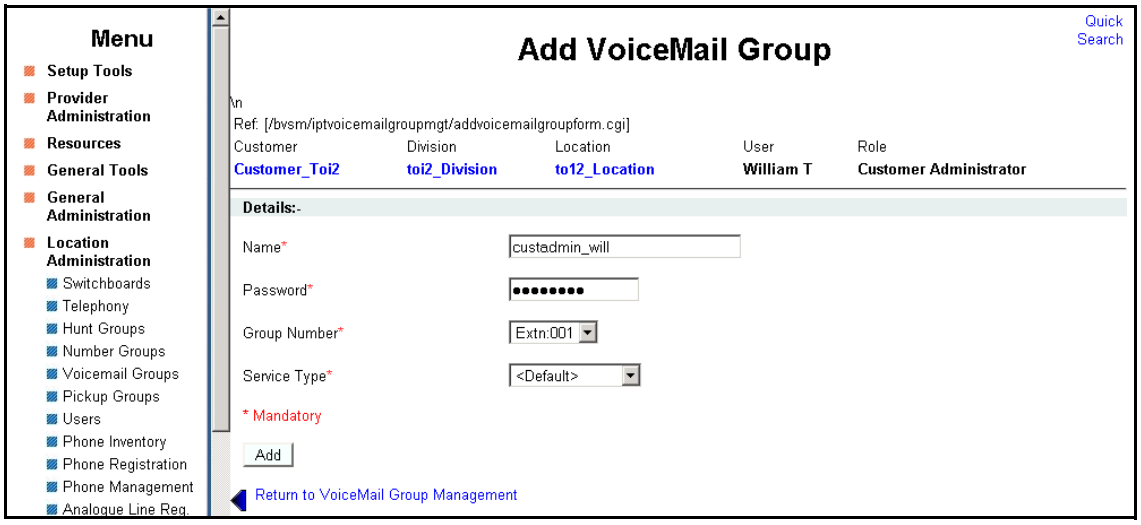
This page displays a list of the voicemail groups in the current location. You can use this page to search for voicemail groups in the database, to manage a specific voicemail group, or add a voicemail group.

Step 2 To manage an existing voicemail group, click the blue link in the Name column.

Step 3 To add a voicemail group, click **Add**.

The screen shown in Figure B-22 appears.

Figure B-22 Add VoiceMail Group



Step 4 Enter the information required for the voicemail group.

Step 5 Select the options required to configure the voicemail group from the pull-down selection lists.

Step 6 Click **Add**.

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, "Location Administration."

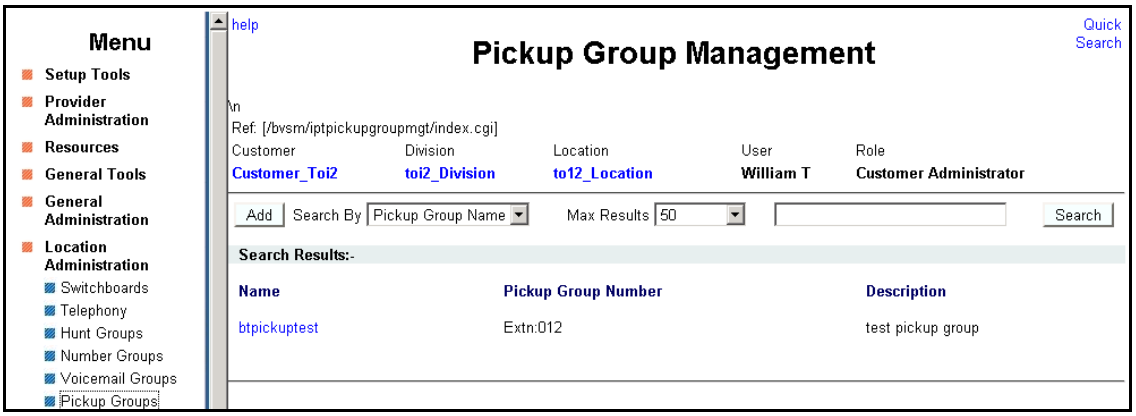
To create a pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

The Pickup Group Management page appears (see Figure B-23).

Figure B-23 Pickup Group Management

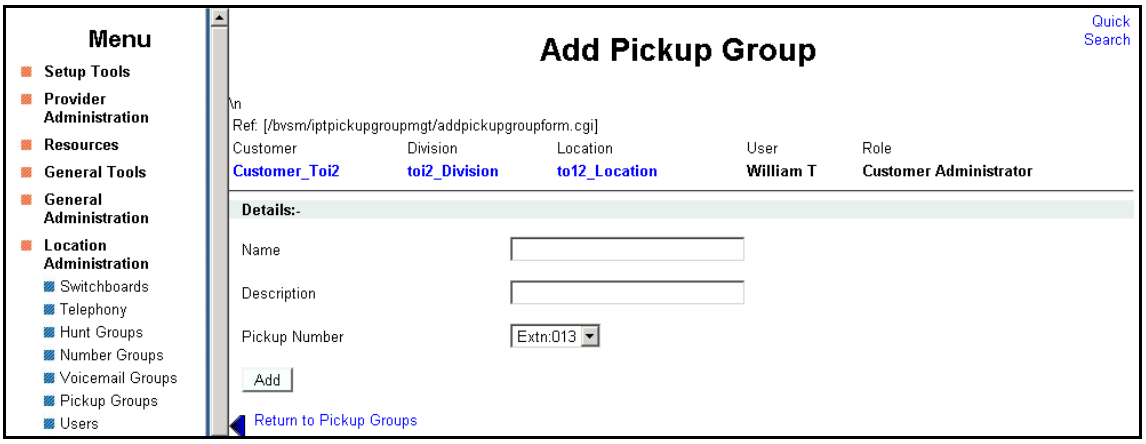


To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add** on the Pickup Group Management page.

The Add Pickup Group page appears (see Figure B-24).

Figure B-24 Add Pickup Group



Step 3 Enter a unique name for the pickup group.

Step 4 (Optional) Enter a description for the pickup group.

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 permissions for users within a location. For information about creating and managing user accounts, refer to Appendix A, “Location Administration.”

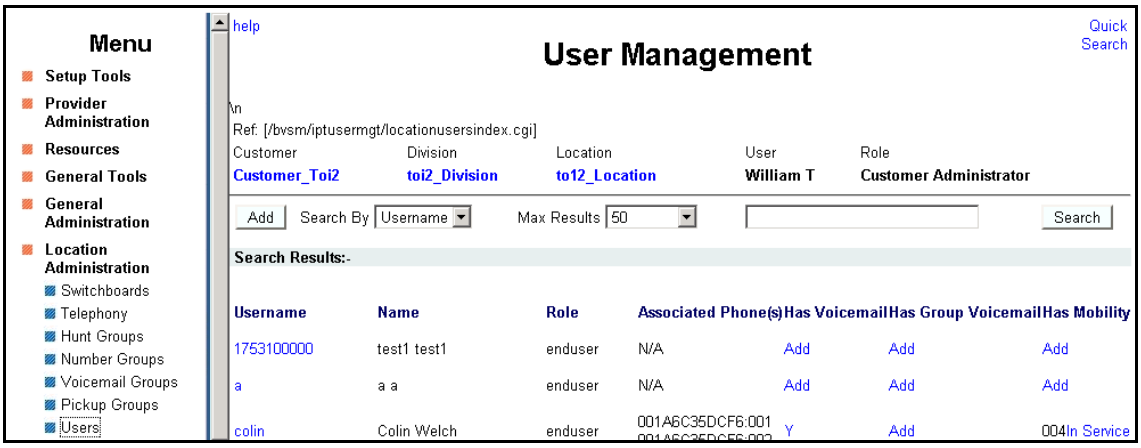
To change the permissions for a user, complete the following steps:

Procedure

Step 1 Click **User Management** on the Location Administration menu.

The screen shown in Figure B-25 appears.

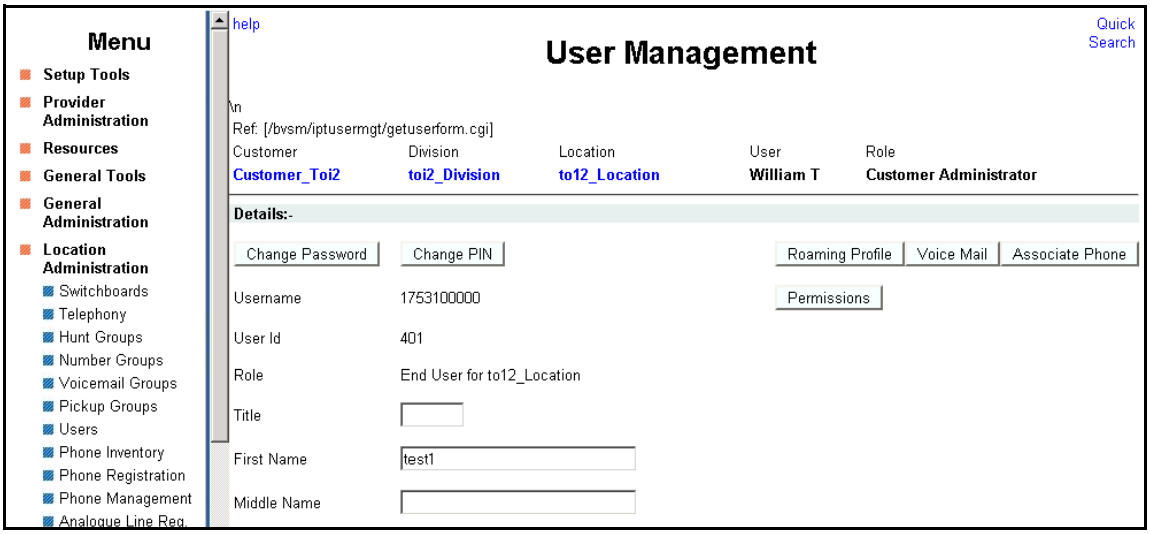
Figure B-25 Location/User Management



Step 2 Click the blue link in the Username column for the user account you want to manage.

The screen shown in Figure B-26 appears.

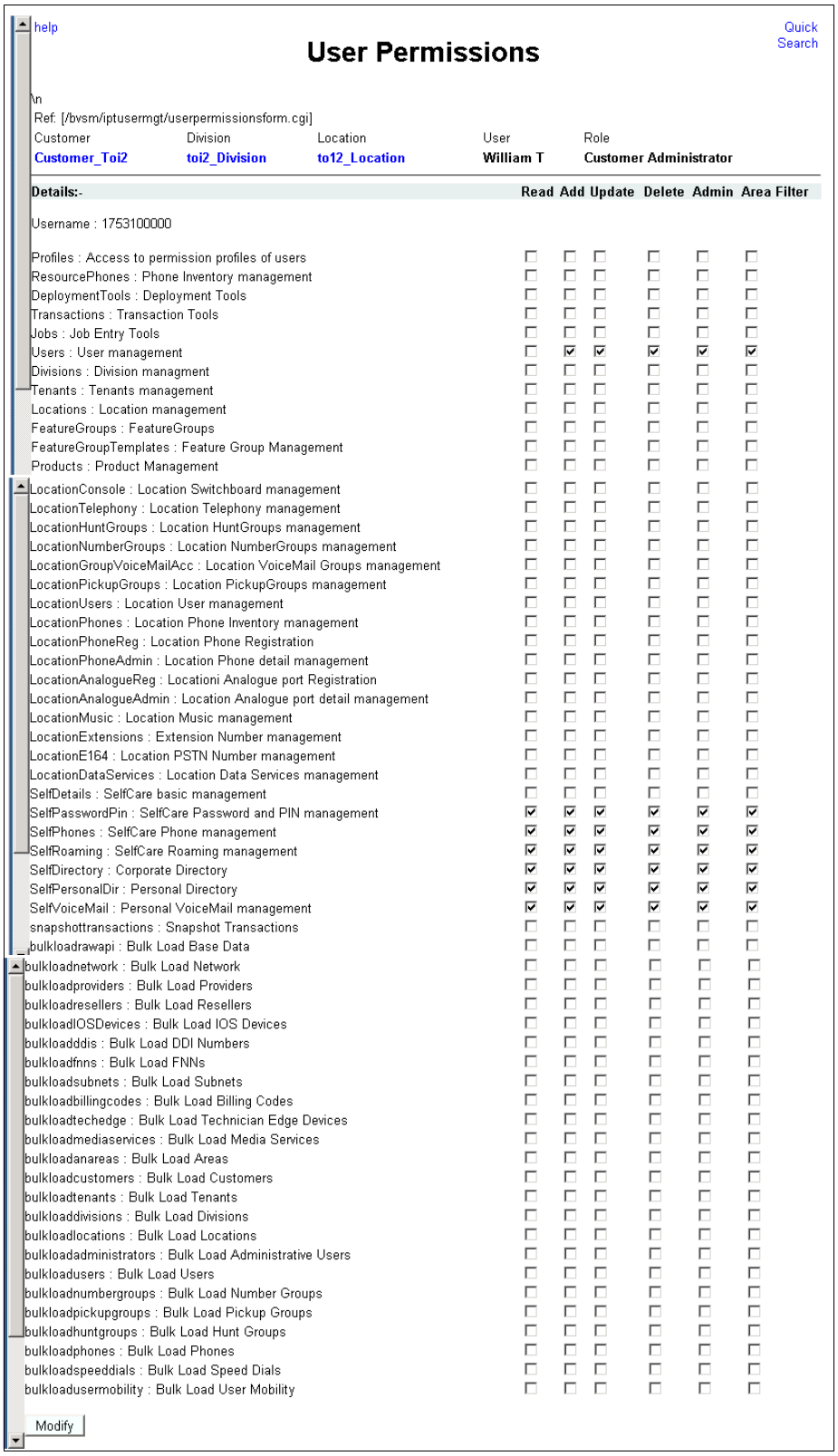
Figure B-26 Location/User Management—Page 2



Step 3 Click **Permissions**.

The screen shown in Figure B-27 appears.

Figure B-27 User Permissions



Note If you change these permissions, the user may be unable to access the affected services. Do not make any changes without carefully considering the consequences.

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 Registration

After a phone is assigned to a location it is assigned its IP address and will appear in the BVSM 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.

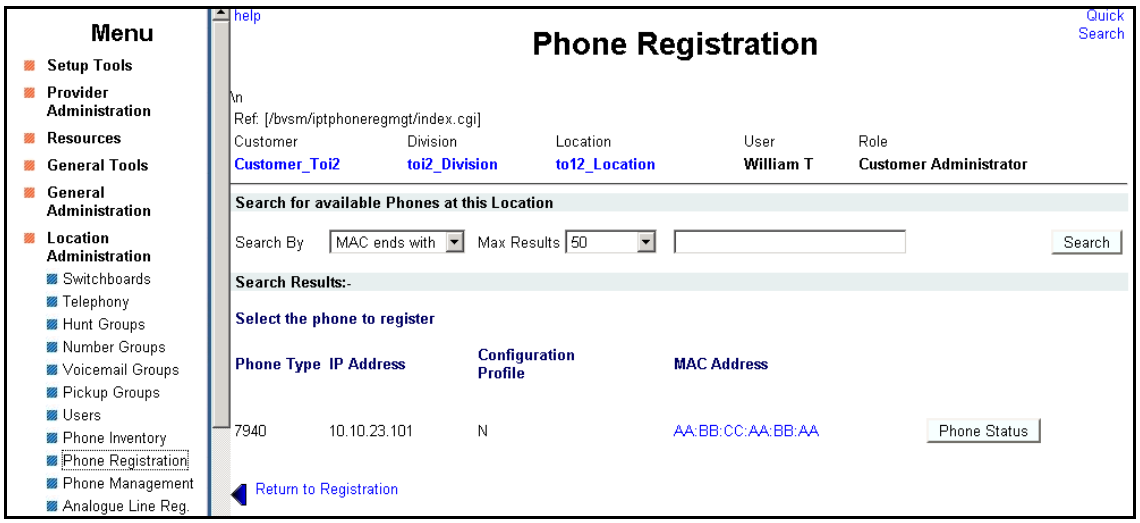
To register phones, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration Menu.

The screen shown in Figure B-28 appears.

Figure B-28 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.

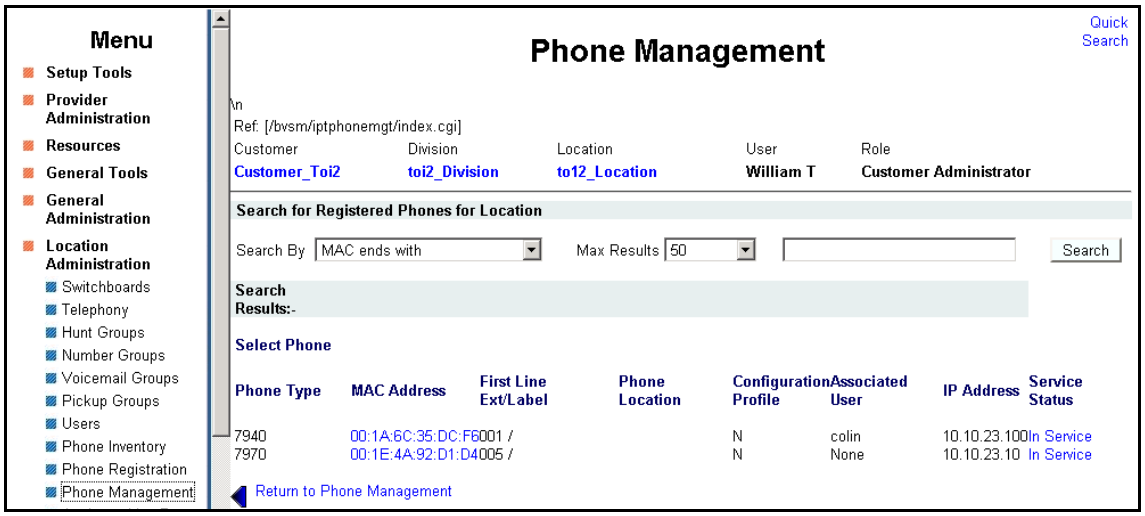
Step 2 To register a phone, click the blue link in the Name column.

For further information about registering phones, see Appendix A, "Location Administration."

Phone Management

Use the **Phone Management** option (Figure B-29) 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."

Figure B-29 Phone Management



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.

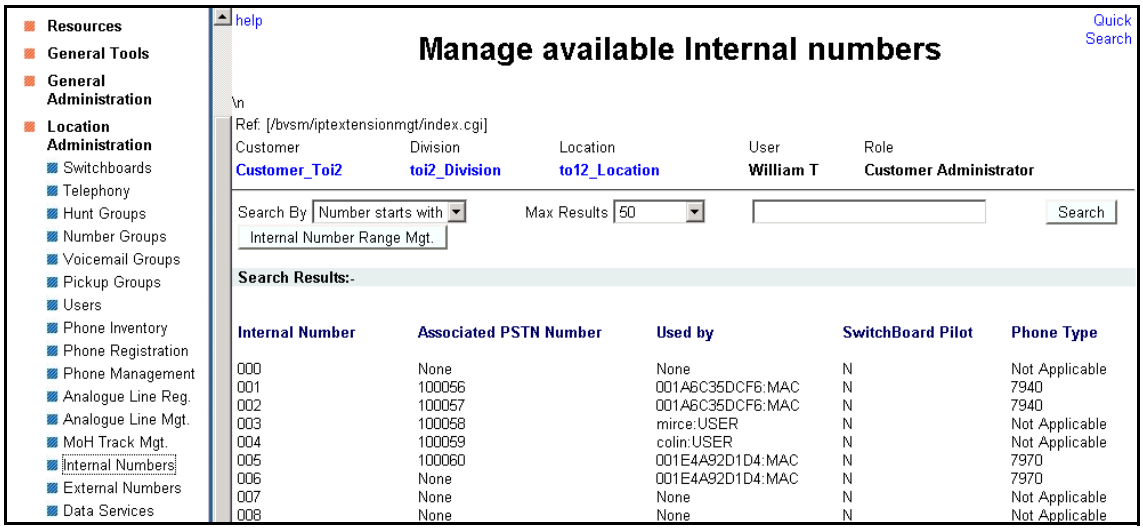
Use the **Internal Numbers** option on the Location Administration menu to manage internal numbers. To manage internal numbers, complete the following steps:

Procedure

Step 1 Select **Internal Numbers** on the Location Administration Menu.

The screen shown in Figure B-30 appears.

Figure B-30 Manage available Internal numbers



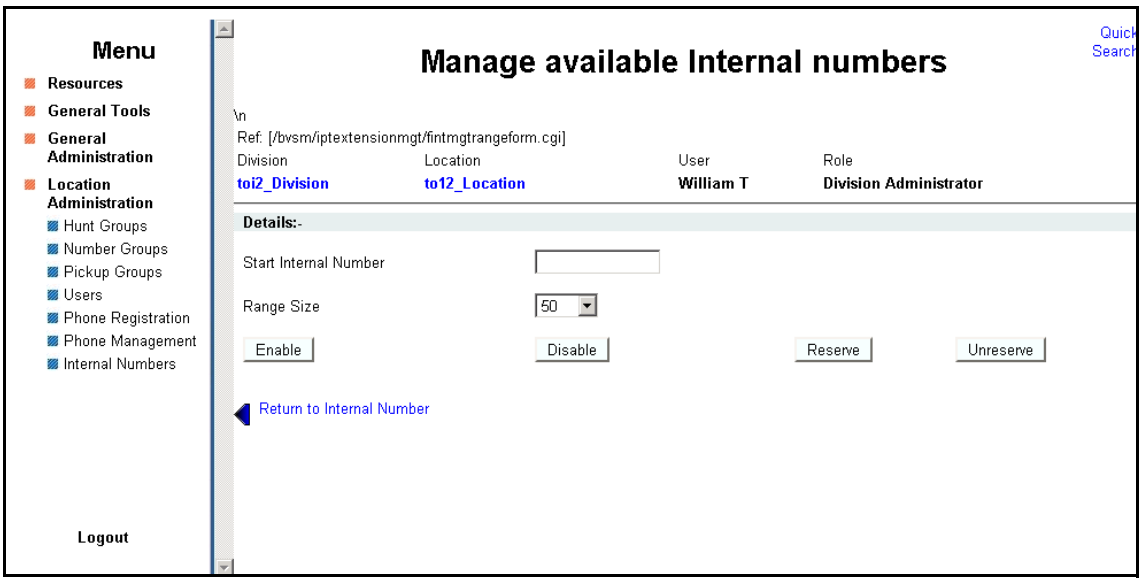
The Manage available internal numbers page provides a list of internal numbers, their associated PSTN numbers, their associated phone users, switchboard pilot, and type of phone. You can use this page to search for internal numbers in the database, or to manage the internal number range.

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.**

The screen shown in Figure B-31 appears.

Figure B-31 Internal Number Range Management



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

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:

- Setup Tools, page C-10
- Provider Administration/Feature Templates, page C-13
- Resources/Phone Inventory, page C-15
- General Tools, page C-18
- General Administration, page C-22
- Location Administration, page C-40

Note For additional information about using the options on the Location Administration menu, refer to Appendix A, Hosted UCS Location Administration. For information about using the options on the Self Care menu, see *Customizing Your Cisco Unified IP Phone: For Cisco Hosted Unified Communications Services, Release 5.1(b).*

Overview

This section includes the following topics:

- User Interface Guidelines, page C-2
- Provisioning Guidelines, page C-4
- Managing Phones, page C-5
- Managing Internal and External Numbers, page C-8
- Managing Services, page C-9
- Using the Pilot Number, page C-10

User Interface Guidelines

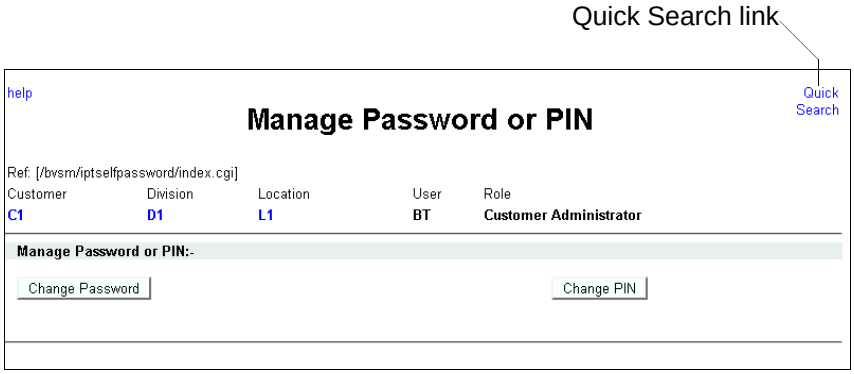
Note the following conventions used in Hosted UCS menus and associated administration pages:

- 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

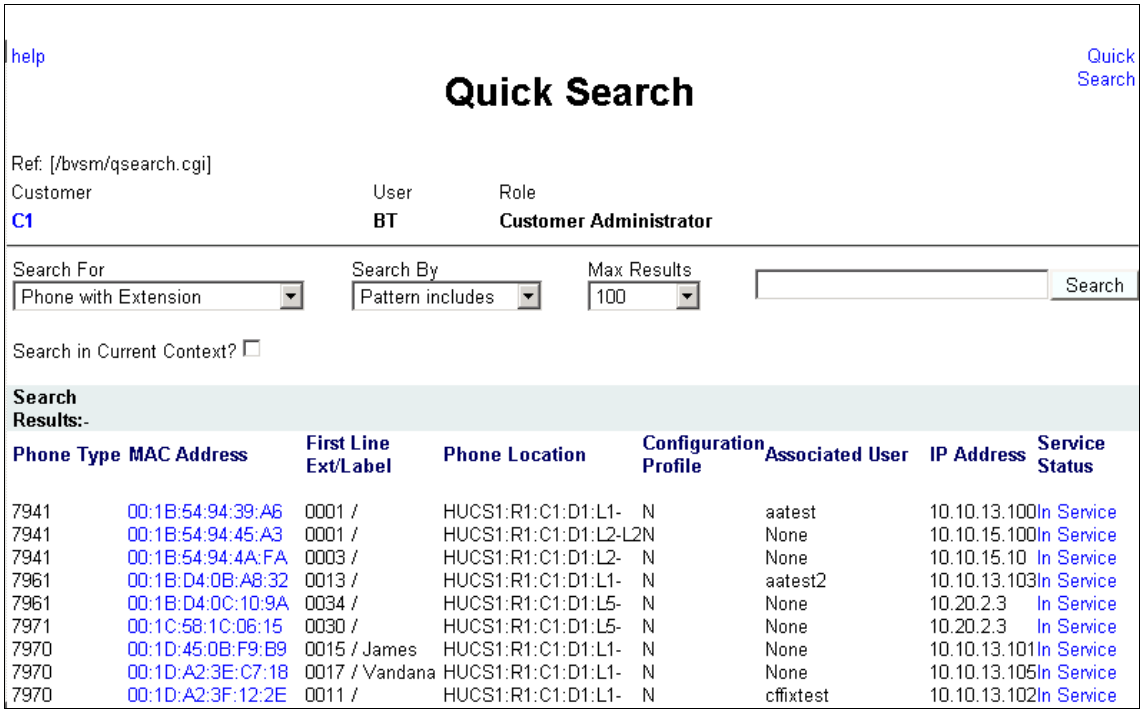
As shown in Figure C-1, each page of the BVSM user interface includes a Quick Search link, which allows you to search the database for specific entries, including phones, extensions, and user accounts. The Quick Search page lets you search for entries of various types from a single page. The entries 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 C-1 Quick Search Link



When you click the Quick Search link, the system displays the page shown in Figure C-2

Figure C-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 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.

Table C-1 Search Types

Search Type	Description
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.

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 "Deployment Tools" section on page C-18).

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-42). 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-5
- Manually Adding Phones, page C-5
- Removing Phones, page C-6
- Autoprovisioning, page C-6

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 BVSM 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 BVSM 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 BVSM.

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.

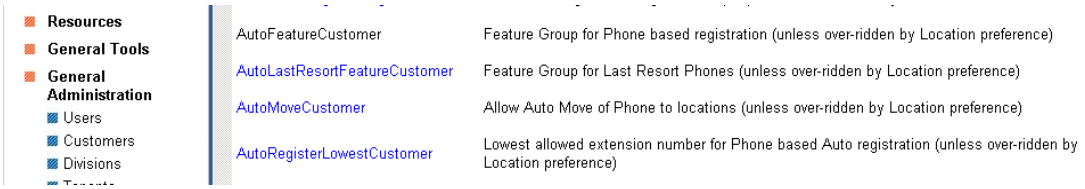
The Hosted UCS system applies a default feature group and selects the lowest number from the internal number pool (with associated DDI if appropriate) to register the phone. The result is that an approved phone can be connected to any office within the correct location and the phones are automatically 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.

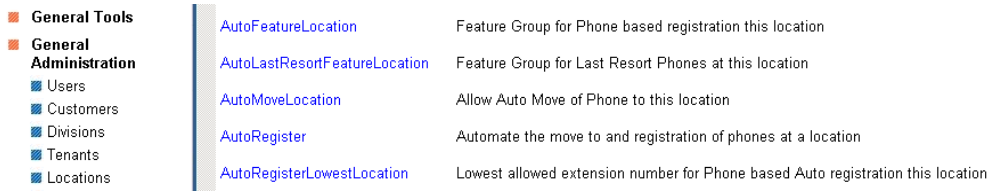
There are four customer settings for Autoprovisioning, as shown in Figure C-3. These settings must be set by the provider administrator when the customer is created.

Figure C-3 Customer Preferences for Autoprovisioning



There are five Location settings for Autoprovisioning, as shown in Figure C-4.

Figure C-4 Location Preferences for Autoprovisioning



To display these settings, click **Preferences** on the Location Management page (see the "Locations" section on page C-27). 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 BVSM 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 BVSM. 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 BVSM server (providing the MAC address of the phone and IP address of the edge router)
   - BVSM identifies the location of the phone by reference to the list of IP addresses loaded into BVSM 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.
   - BVSM 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.
   - BVSM 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, BVSM 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 BVSM. 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. BVSM 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. BVSM 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 the following options available on the Setup Tools menu:

- Samples, page C-11

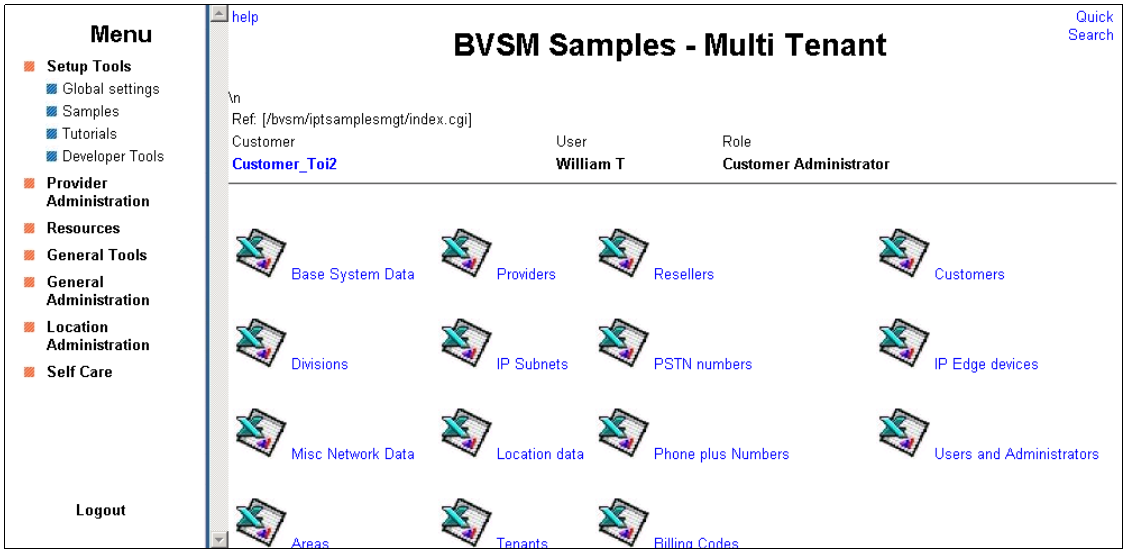
- Developer Tools, page C-11

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.

The screen shown in Figure C-5 appears.

Figure C-5 Samples

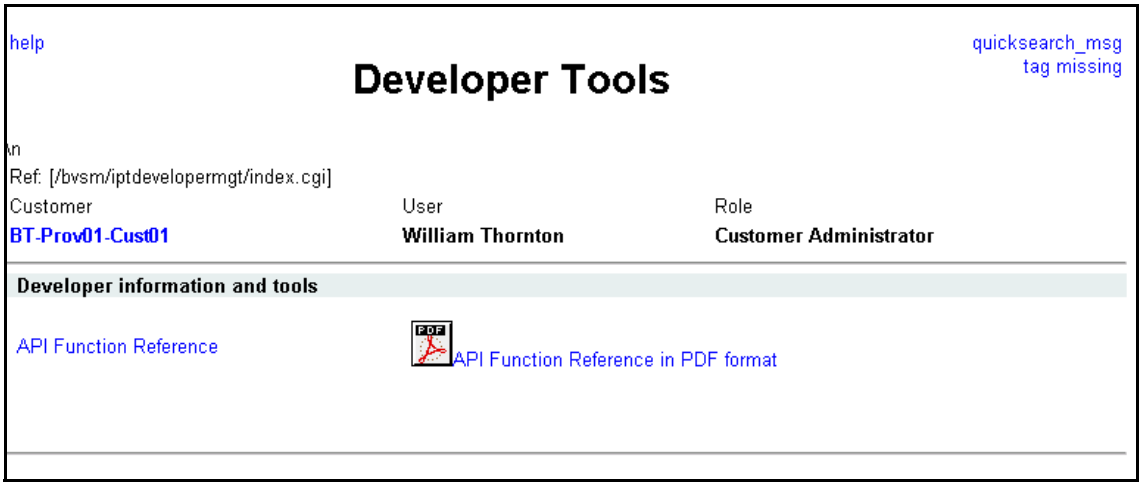


Developer Tools

To option a PDF copy of the *API Functional Reference* guide, select the **Developer Tools** option on the Setup Tools menu.

The screen shown in Figure C-6 appears.

Figure C-6 Developer tools

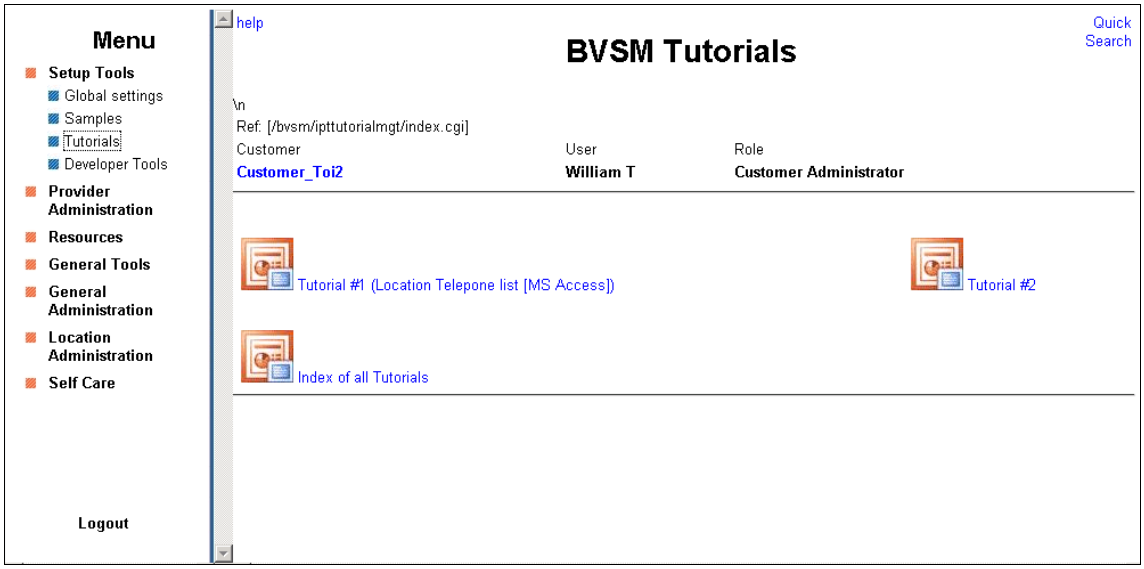


Tutorials

To view Powerpoint presentations, providing tutorial examples of how to use the Hosted UCS user interface, select the **Tutorials** option on the Setup Tools menu.

The screen shown in Figure C-7 appears.

Figure C-7 Tutorials



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.

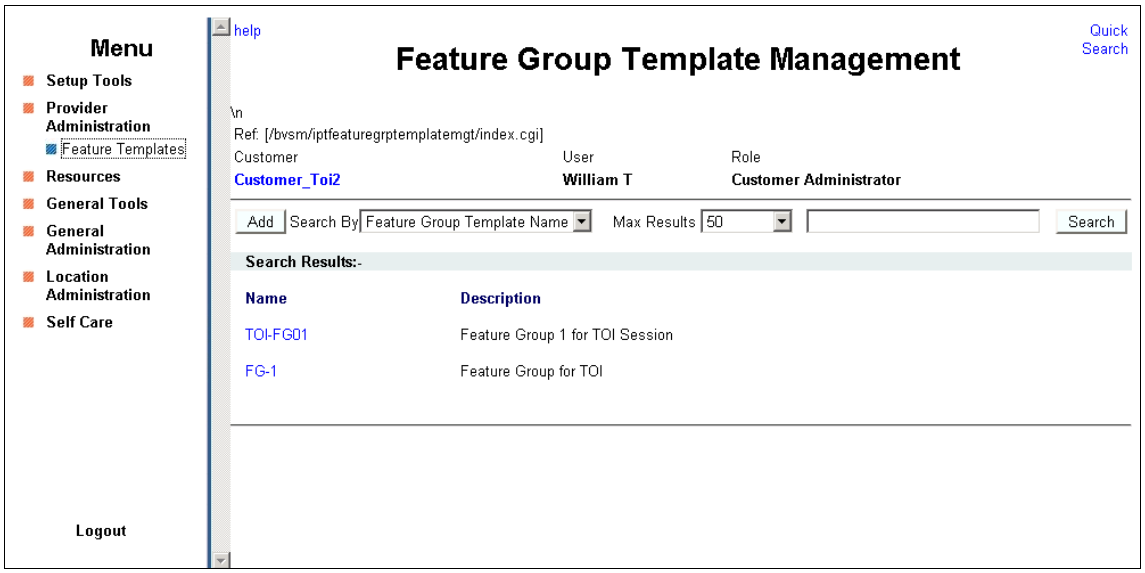
To create a feature group, complete the following steps:

Procedure

Step 1 Click Feature Templates on the Provider Administration menu.

The screen shown in Figure C-8 appears.

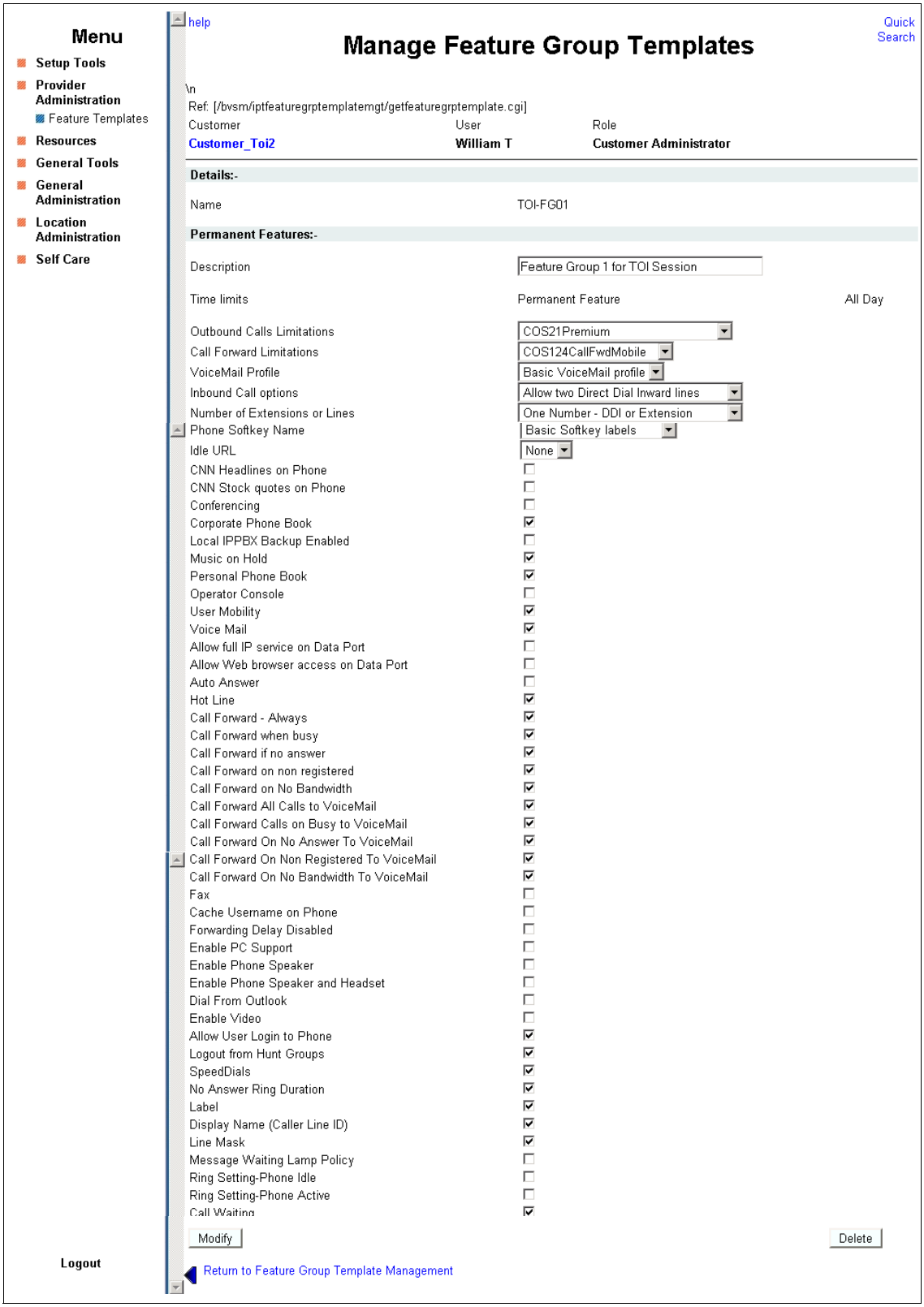
Figure C-8 Feature Group Template Management



Step 2 To create a feature group template, click **Add**.

The screen shown in Figure C-9 appears.

Figure C-9 Feature Group Template Management



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.

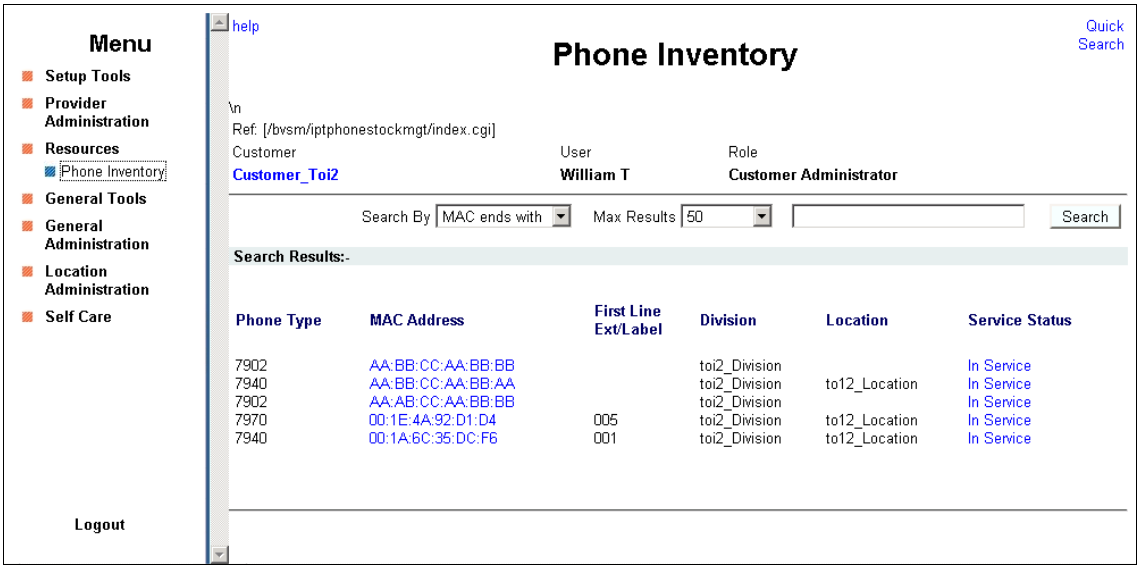
To view the phone inventory or move a phone between locations, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the Resources Menu.

The screen shown in Figure C-10 appears.

Figure C-10 Phone Inventory



This page provides a list of the phones on the system with their location and status. To search for a phone, select one of the following options from the Search by pull-down selection list:

- MAC starts with

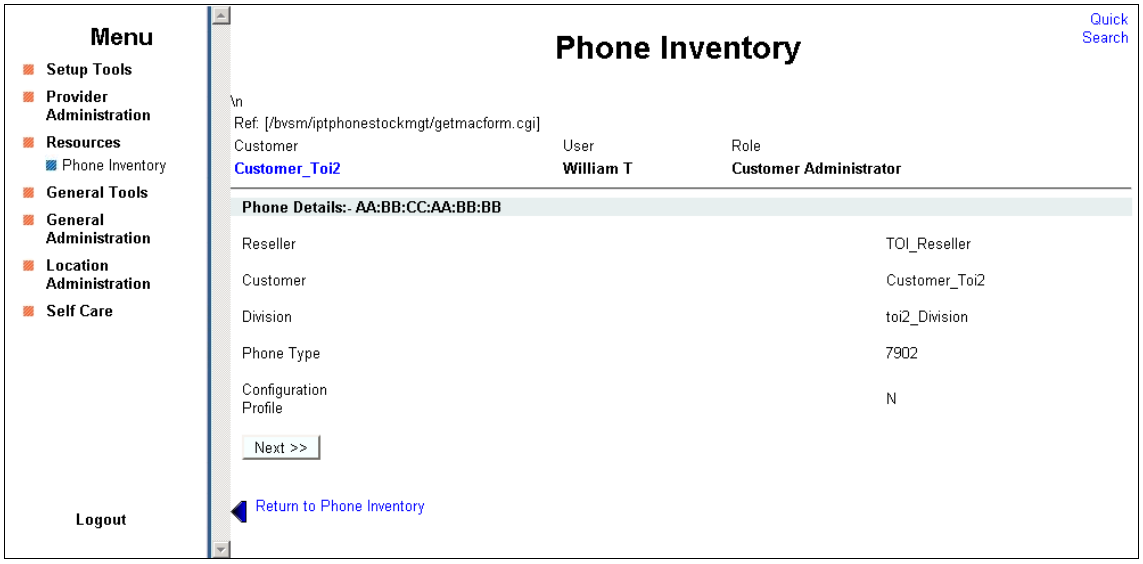
- MAC ends with
- Search by phone location
- Extension Number Ends with
- Extension Number Starts with
- Full Internal Number

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.

The screen shown in Figure C-11 appears.

Figure C-11 Allocate/Move Phone—Page 1



This page lists information about the selected phone and lets you move it to a different location.

Step 3 Click **Next**.

The screen shown in Figure C-12 appears.

Figure C-12 Allocate/Move Phone—Page 2

Step 4 Select the location to which you want to move the phone from the pull-down selection list.

Step 5 Click **Next**.

The screen shown in Figure C-13 appears.

Figure C-13 Allocate/Move Phone—Page 3

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.

- Deployment Tools, page C-18
- Transactions, page C-19
- Basic Reports, page C-20

Deployment Tools

Use the **Deployment Tools** (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.

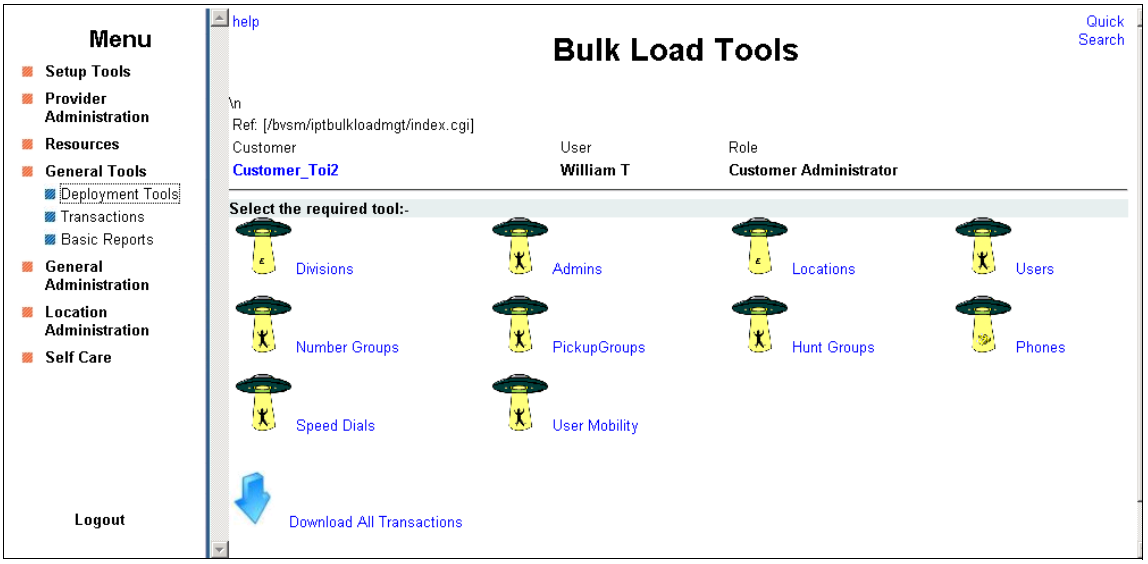
There are three sets of bulk loaders provided with the Hosted UCS platform:

- Dial plan model loaders—Including settings for BVSM, and dial plans for Cisco PGW, and Cisco Unified Communications (Unified CM)
- Configuration loaders—Provider, network, and reseller settings
- Customer loaders—Location, user, and phone data settings

Note The first sheet in the Excel workbook containing a bulk loader must contain the BVSM version number. The bulk loader is only uploaded if the version number corresponds to the BVSM version of the Hosted UCS platform.

When you select the **Deployment Tools** option, the screen shown in Figure C-14 appears.

Figure C-14 Deployment Tools



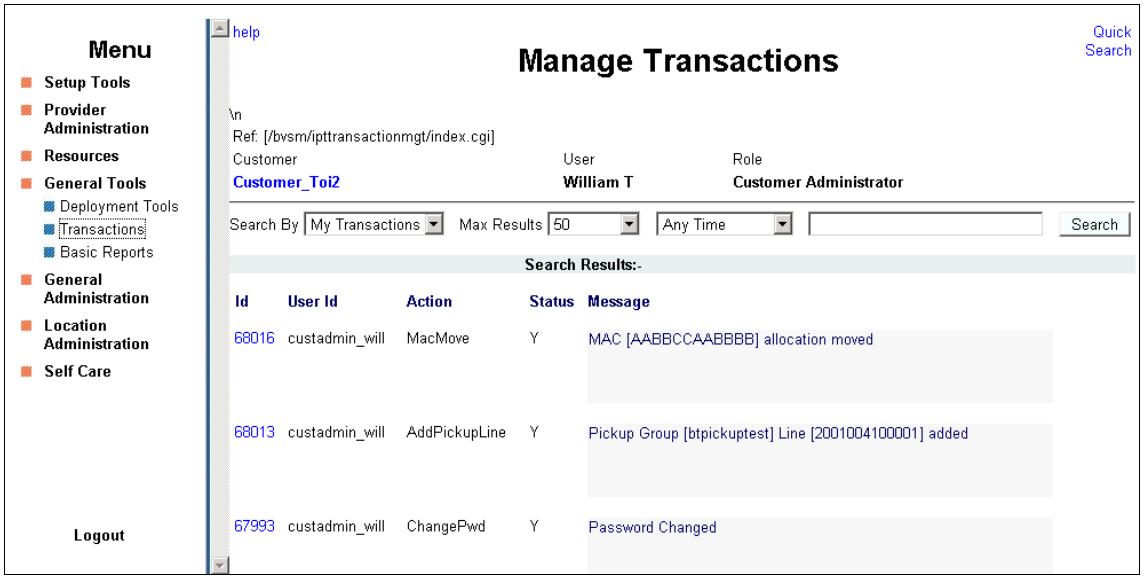
This page displays the bulk data loaders available on your system. For further information about using bulk data loaders, see *Getting Started with Hosted Unified Communications Services*, at the following website:

http://www.cisco.com/en/US/docs/voice_ip_comm/hucs/5_1b/english/user/guide/HUCS_bk.pdf

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 C-15 appears.

Figure C-15 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

Basic Reports

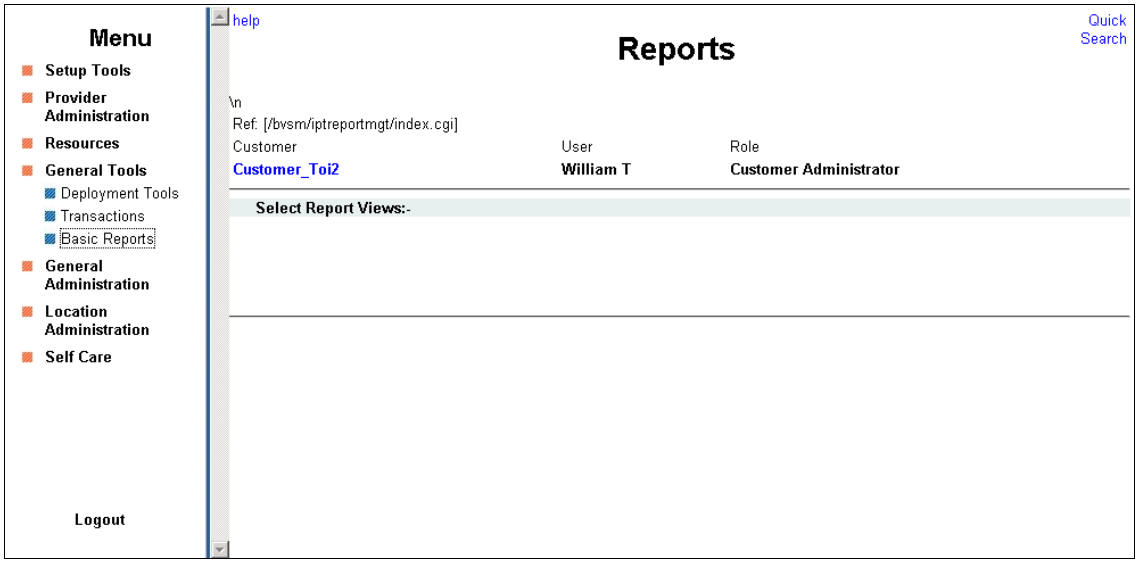
The following is a list of reports that are currently provided with BVSM:

- Directory List (under Self Care menu)
  - First Name
  - Second Name
  - Location
  - Extension Number
  - PSTN Number
- User List (under Location Administration)
  - User ID
  - User Name
  - Role

    - Provider, Reseller, Customer, Division, Locations
- Phone Inventory List (under Location Administration menu)
    - Phone Type
    - MAC Address
    - Reseller, Customer, Division, Locations
    - Registration status
    - IP Address
- Phone Management (under Location Administration)
    - Phone Type
    - MAC Address
    - 1st Line Number
    - Phone Location
    - Associated User
    - IP Address
- Internal Number Inventory (under Location Administration)
    - Internal Number
    - Associated E164 Number
    - Associated Phone/User
    - Switchboard Pilot
    - Phone Type

When you click the **Basic Reports** option, the screen shown in Figure C-16 appears.

Figure C-16 Reports



This page displays a list of the reports available.

Click the blue link in the Select Report Views to view a specific report.

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, page C-22
- Divisions, page C-23
- Tenants, page C-26
- Locations, page C-27
- Feature Groups, page C-37

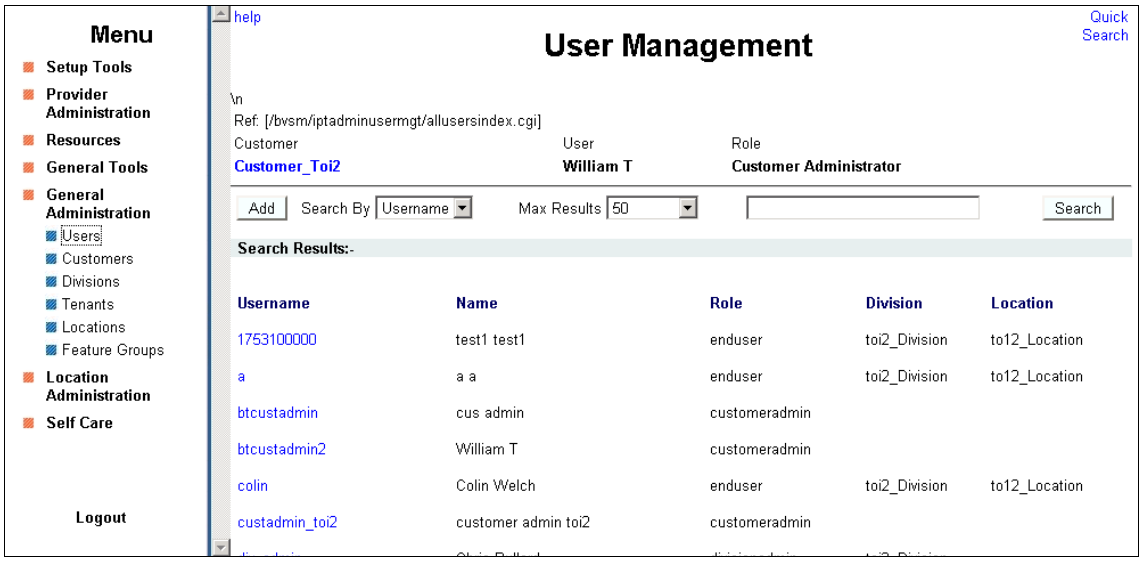
Users

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-50.

Use the **Users** option on the General Administration menu to view information about users across locations.

When you select the **Users** option on the General Administration menu to the screen shown in Figure C-17 appears.

Figure C-17 General Administration/User Management



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:

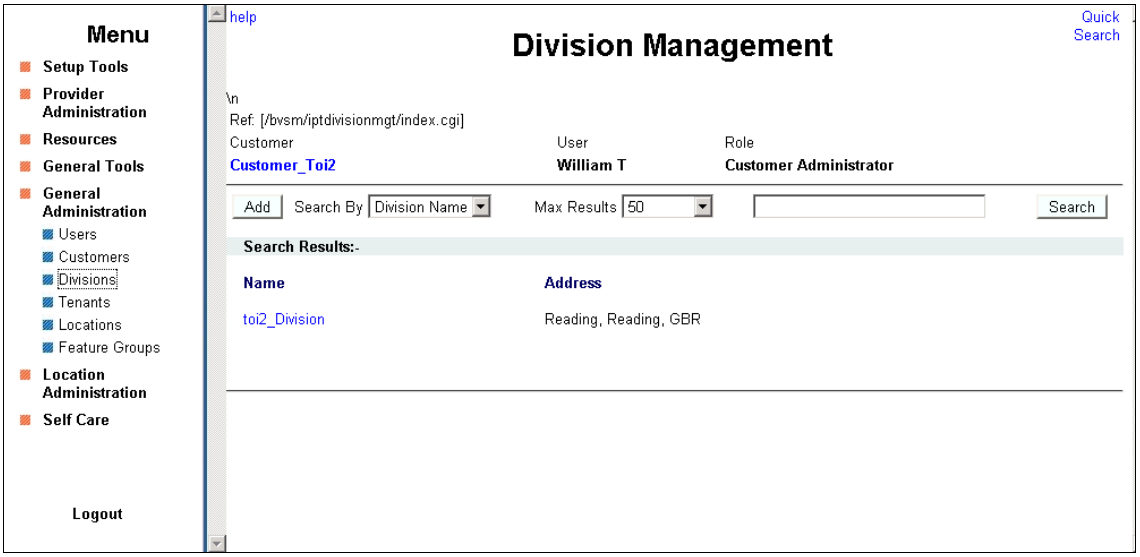
Procedure

Step 1 Select **Division** on the General Administration Menu.

Note If the Division Management page does not appear immediately, click the links on each page until it appears.

The screen shown in Figure C-18 appears.

Figure C-18 Division Management



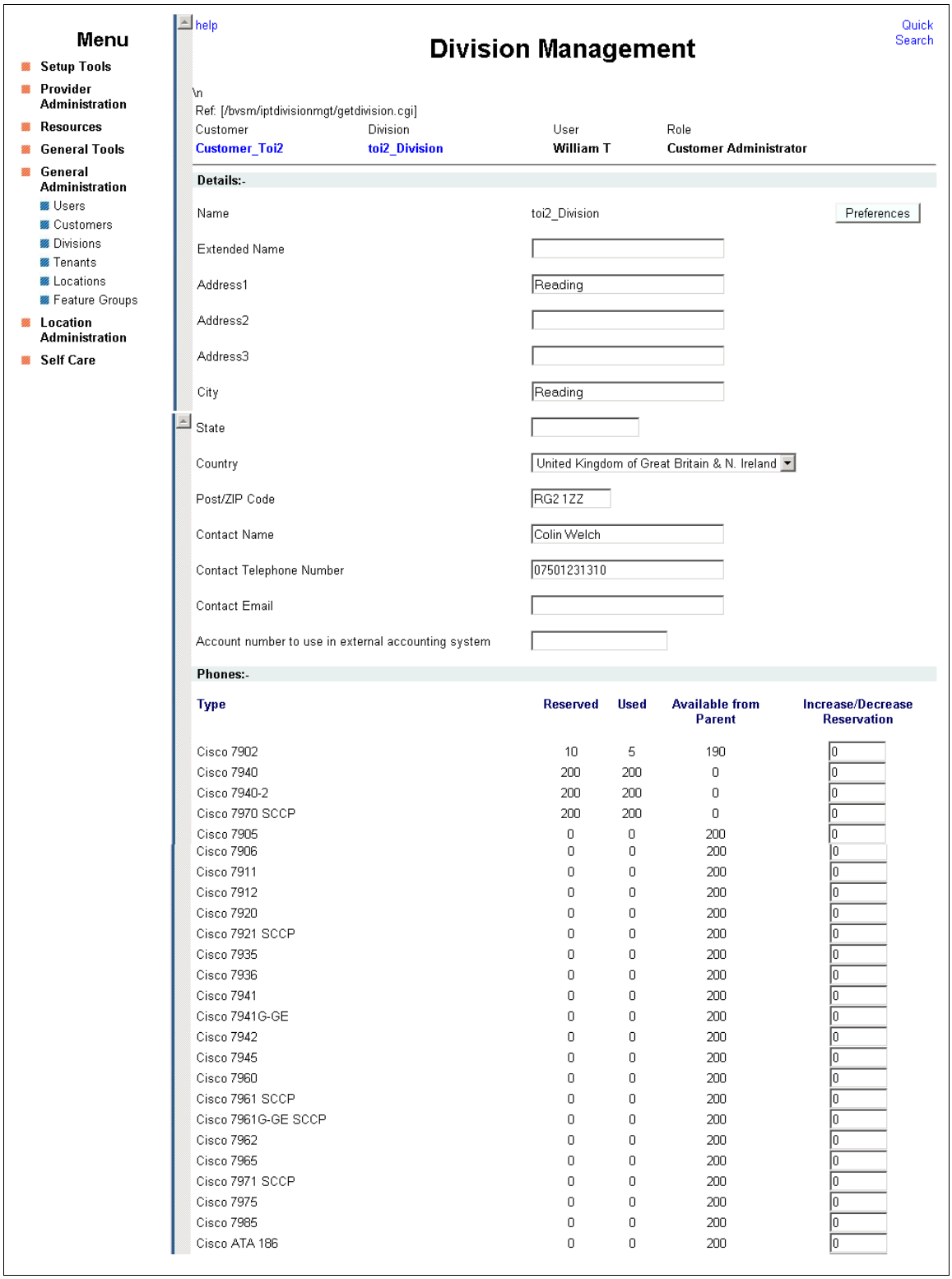
This page displays a list of the divisions in the Hosted UCS system. You can use this page to search for divisions in the database, to manage a specific division, or add a division.

Step 2 To manage an existing division, click the blue link in the Name column.

Step 3 To add a division, click **Add**.

The screen shown in Figure C-19 appears.

Figure C-19 Division Management

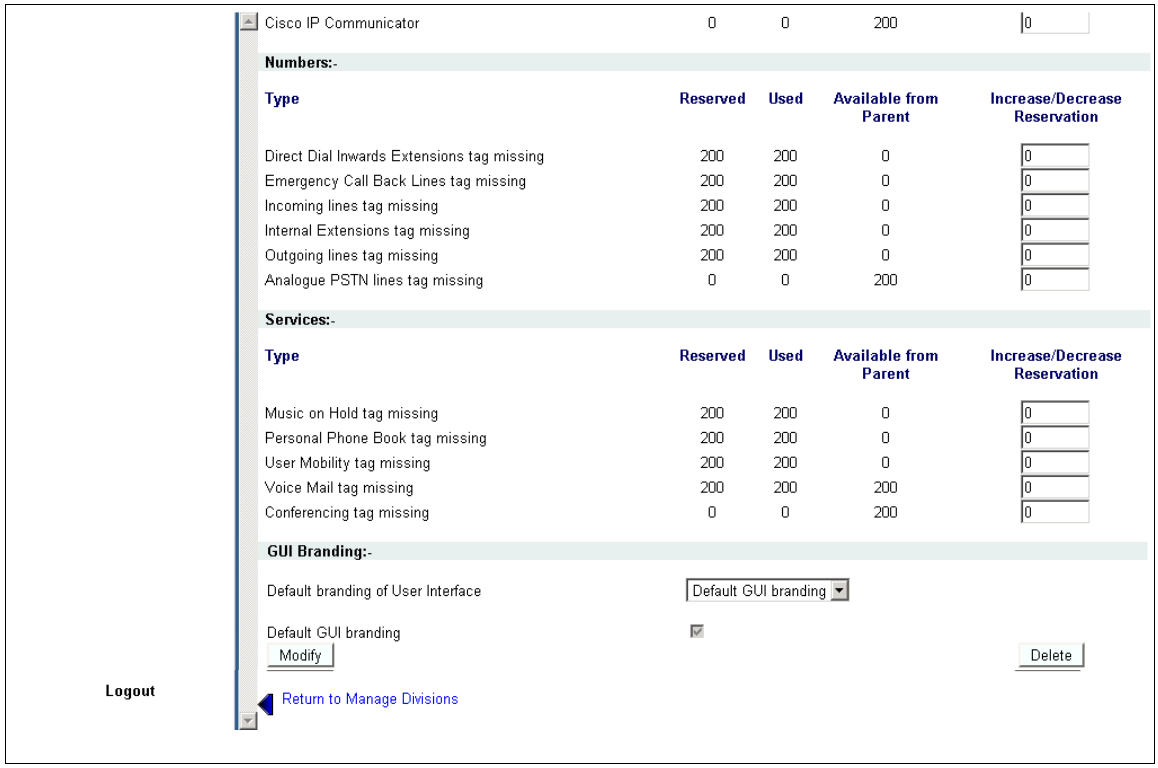


Step 4 Complete any fields required.

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.

Figure C-20 Division Management (continued)



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.

Tenants

A tenant defines a group of phone and users within a single location with its own administration. Use the Tenants option on the General Administration menu to manage existing tenants or to create a new tenant.

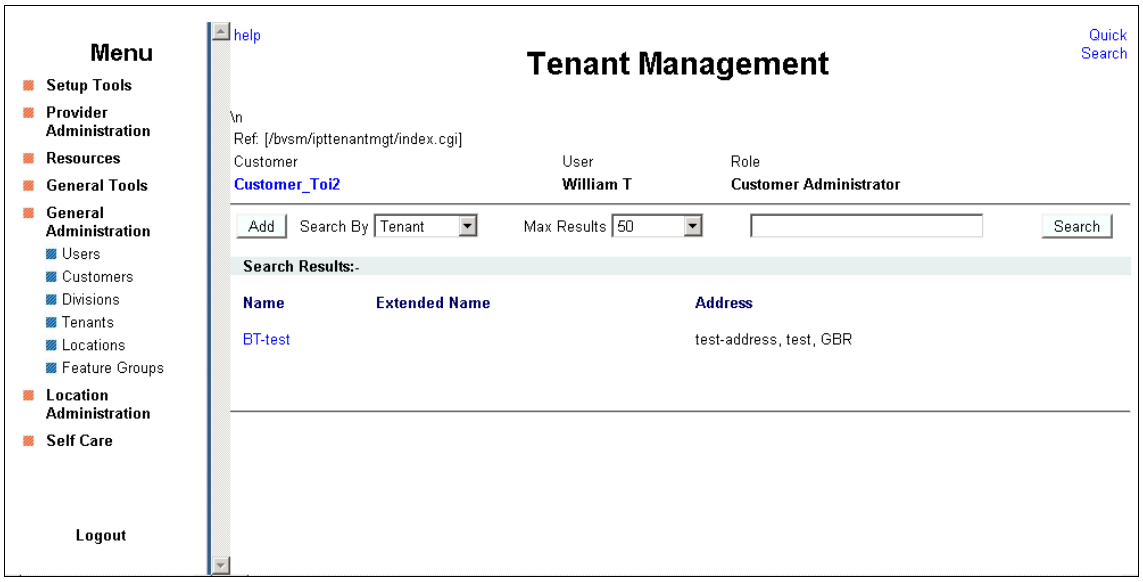
To manage tenants, complete the following steps:

Procedure

Step 1 Select **Tenants** on the General Administration Menu.

The page shown in Figure C-21 appears.

Figure C-21 Tenant Management



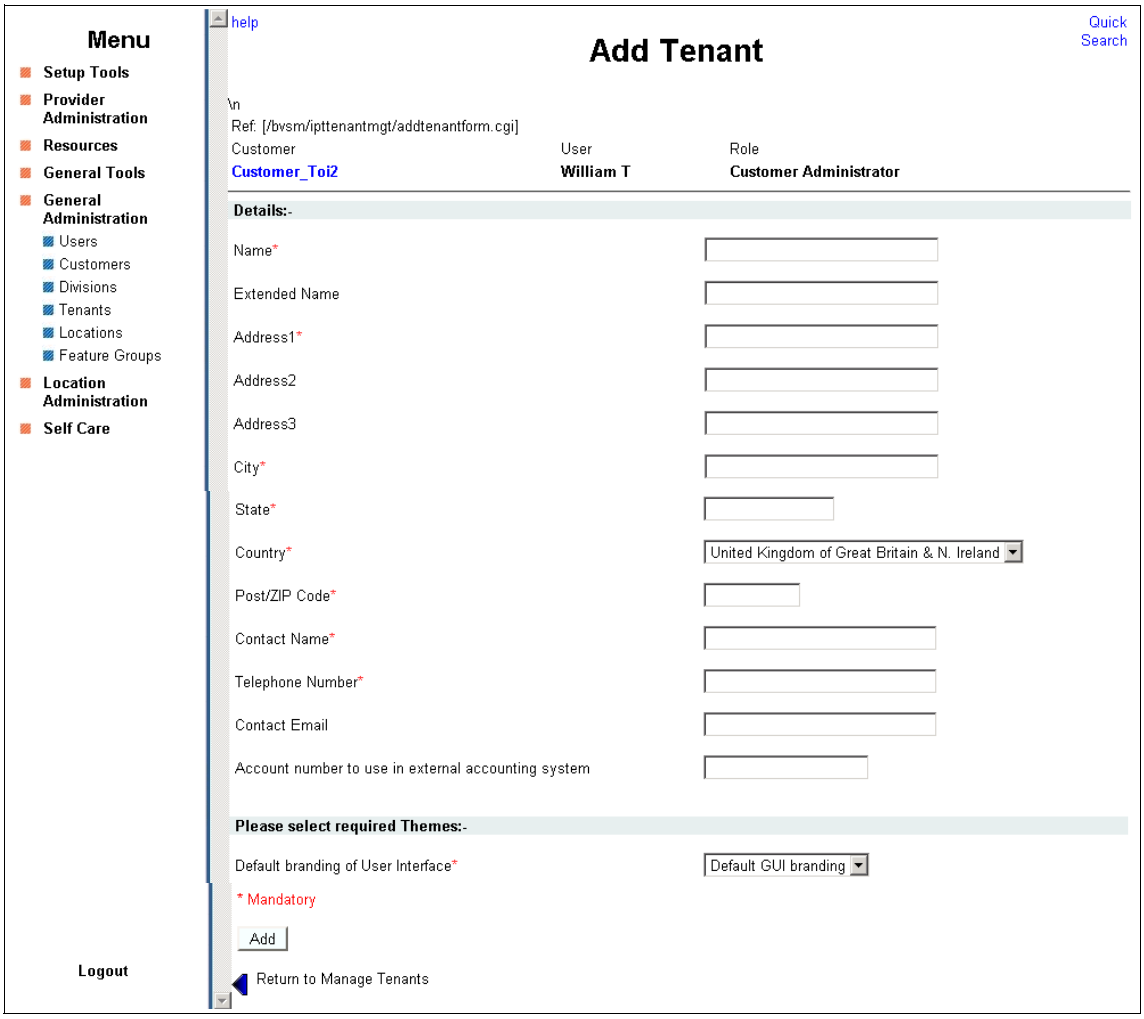
This page displays a list of the tenants in the Hosted UCS system. You can use this page to search for tenants in the database, to manage a specific tenant, or add a tenant.

Step 2 To manage an existing tenant, click the blue link in the Name column.

Step 3 To add a tenant, click **Add**.

The screen shown in Figure C-22 appears.

Figure C-22 Add Tenant



Step 4 Complete any fields required for the tenant.

Step 5 Click **Add**.

The tenant 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.

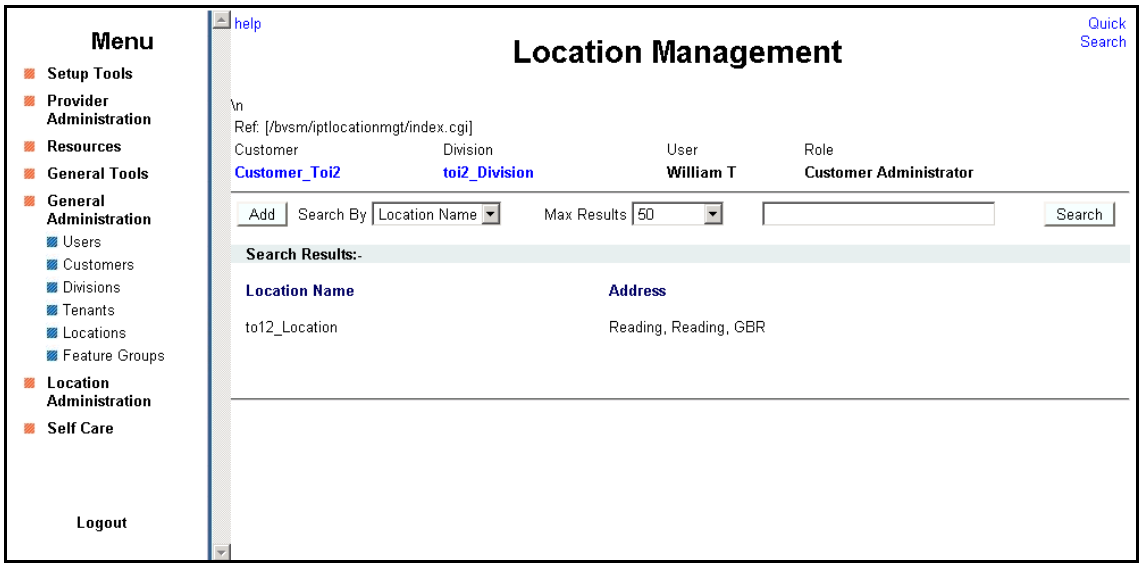
To add a new location, complete the following steps:

Procedure

Step 1 Select **Location** from the Location Administration menu.

The screen shown in Figure C-23 appears.

Figure C-23 Location Management



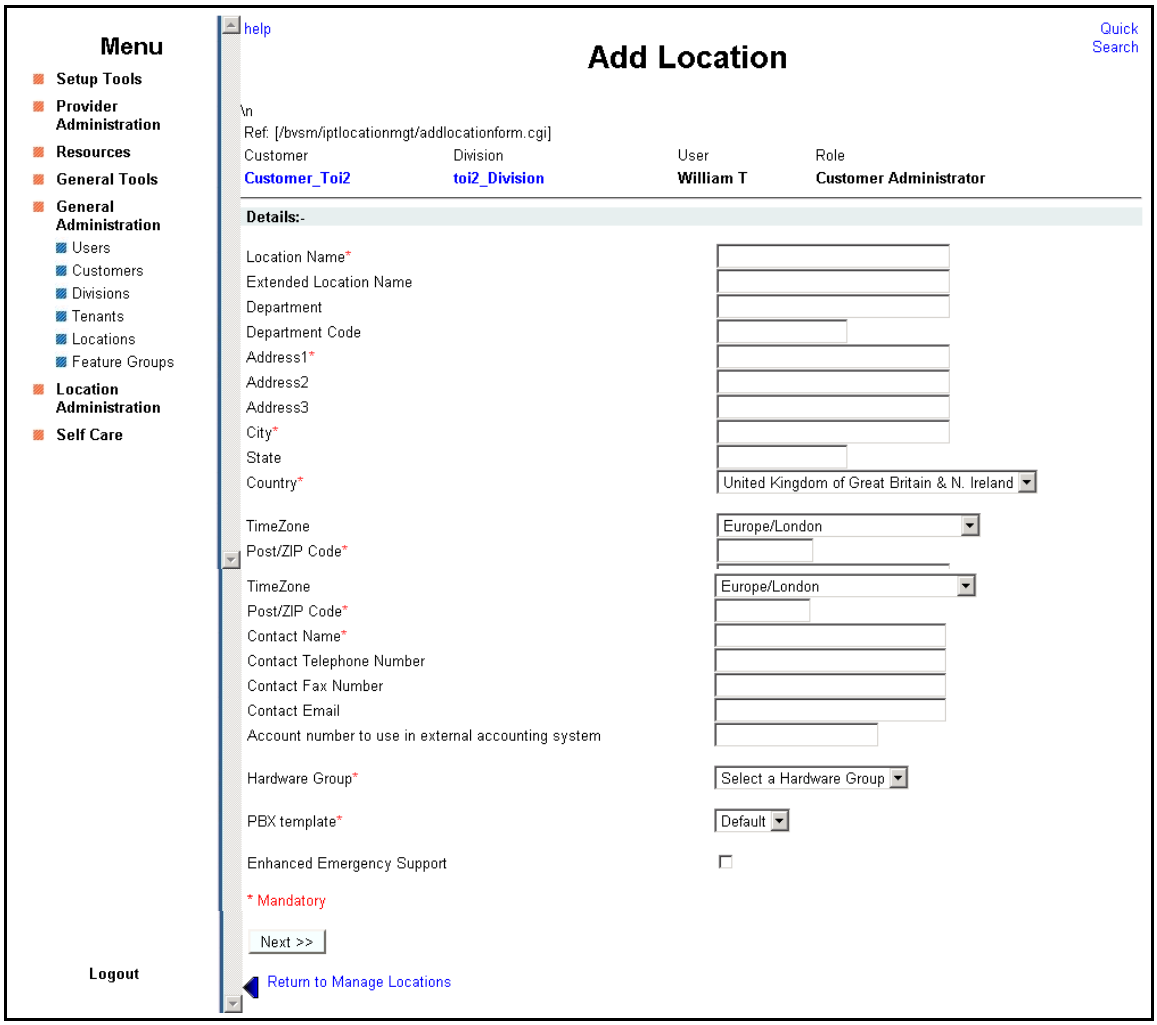
This page displays a list of the locations in the Hosted UCS system. You can use this page to search for locations in the database, to manage a specific location, or add a location.

Step 2 To manage an existing location, click the blue link in the Name column.

Step 3 To add a location, click **Add**.

The screen shown in Figure C-24 appears.

Figure C-24 Add Location



Step 4 Enter the details required for the current location.

The mandatory fields are indicated by a red asterisk.

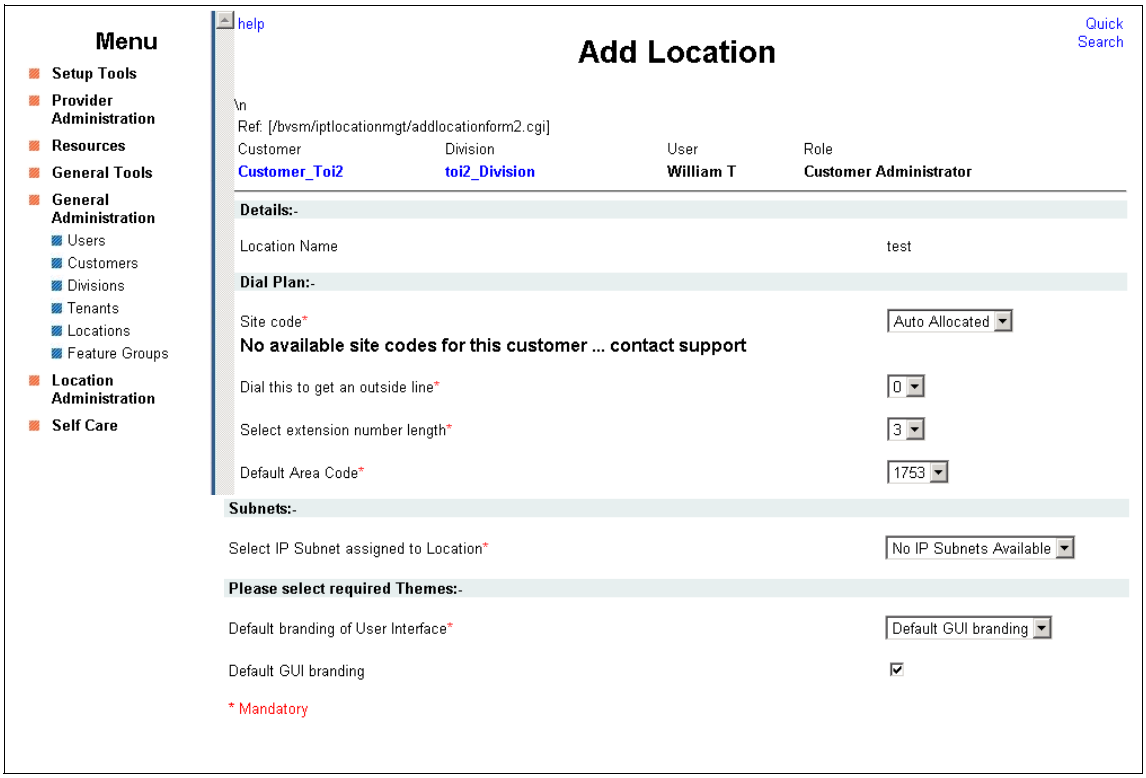
Step 5 Select Hardware Group from the drop-down menu.

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**.

The screen shown in Figure C-25 appears.

Figure C-25 Add Location—Page 2



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.

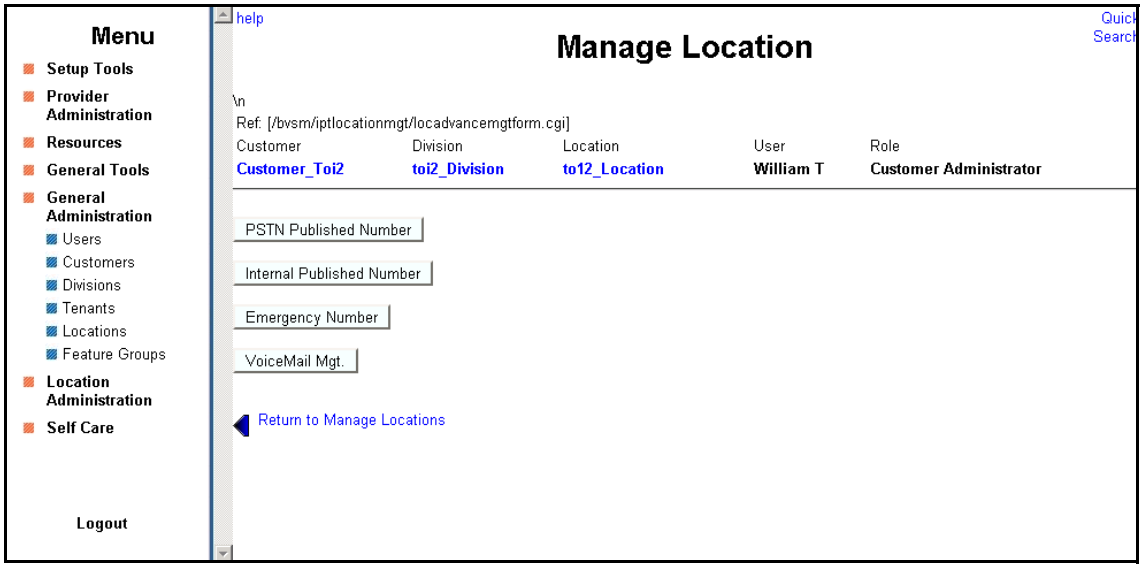
Managing Location Resources

The screen shown in Figure C-26 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.

Figure C-26 Manage Location



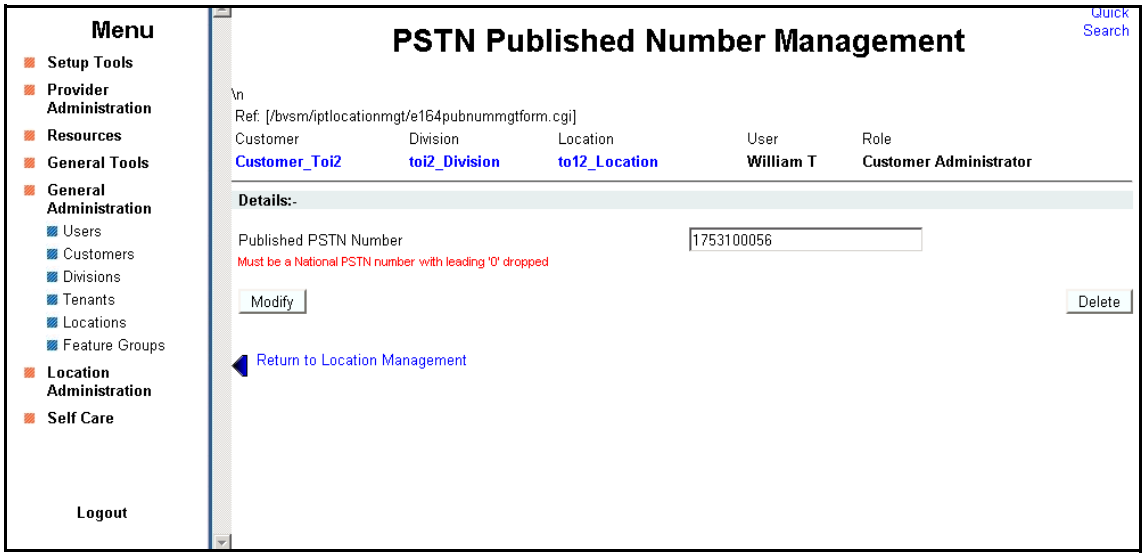
PSTN Published Number

To manage the PSTN numbers for the current location, complete the following steps:

Procedure

Step 1 Click **PSTN Published Number**.

Figure C-27 PSTN Published Number Management



Step 2 Type the PSTN number in the Published PSTN Number field.

Step 3 Click Modify.

Internal Published Number

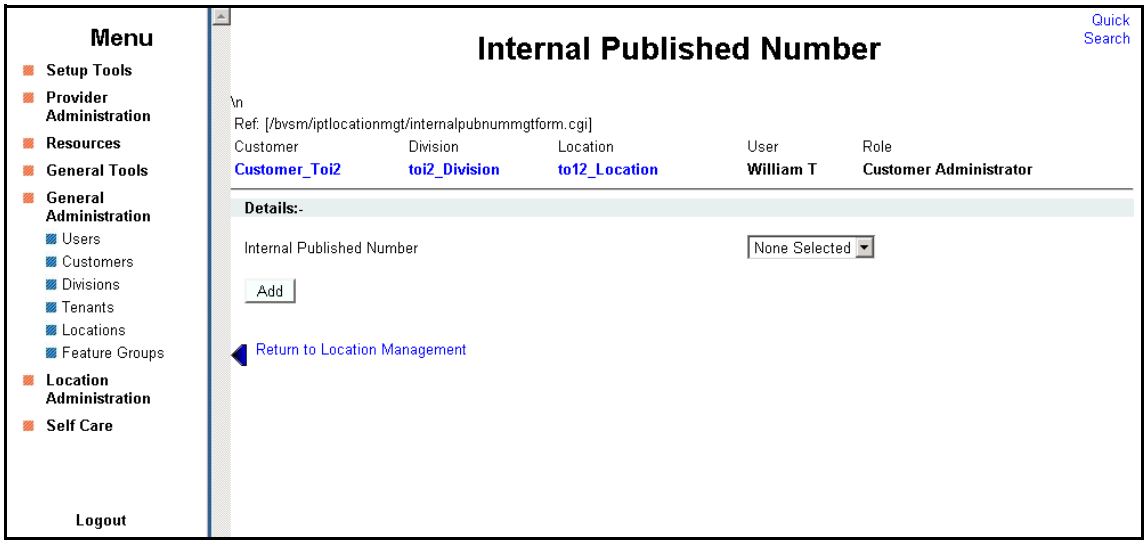
To manage the internal published numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Internal Published Number**.

The screen shown in Figure C-28 appears.

Figure C-28 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

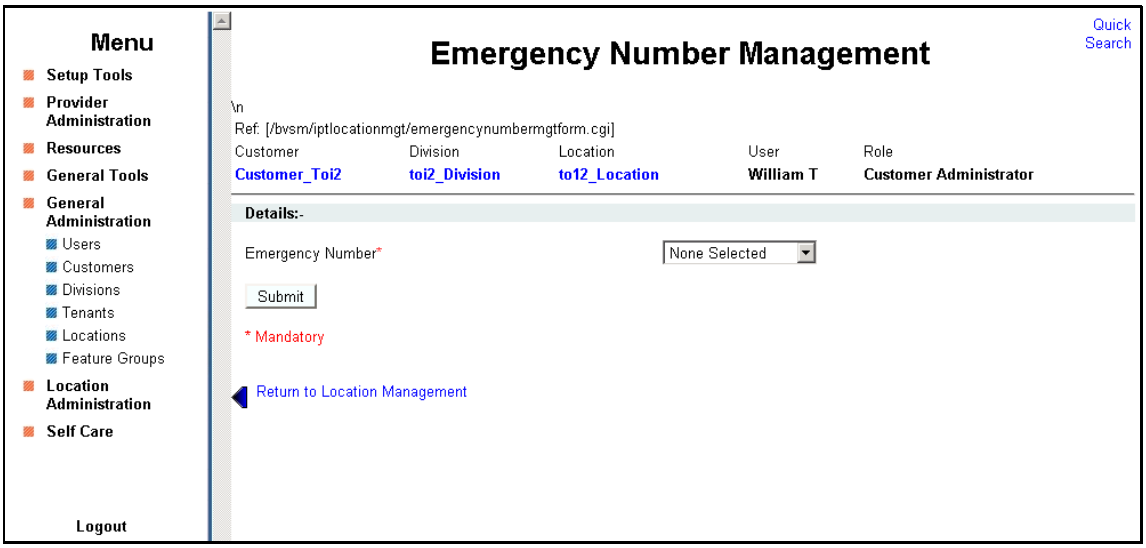
To manage the emergency numbers for the current location, complete the following steps:

Procedure

Step 1 Click **Emergency Number**.

The screen shown in Figure C-29 appears.

Figure C-29 Emergency Number Management



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.

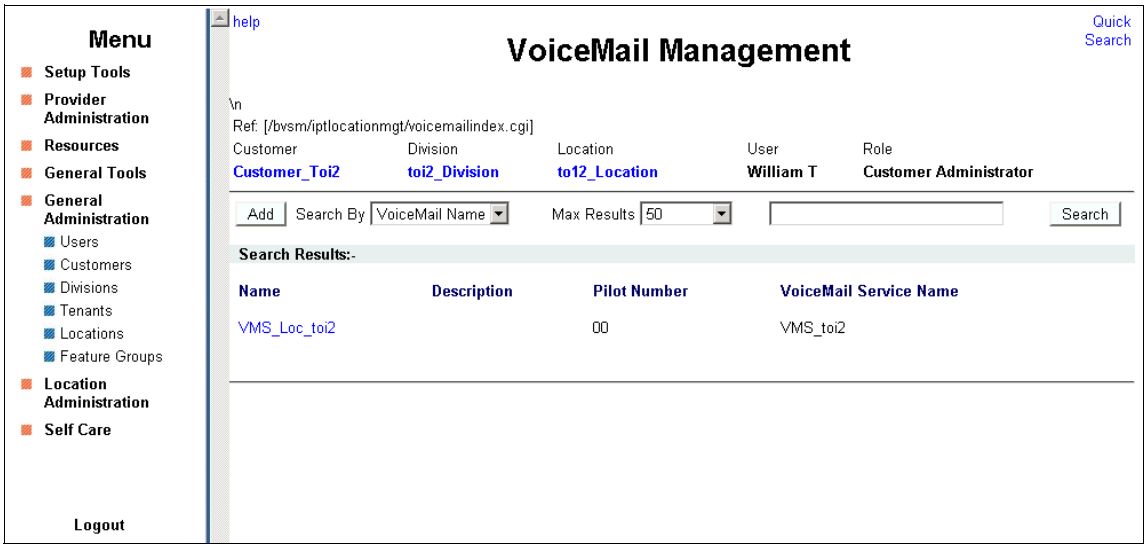
To manage voicemail services, complete the following steps:

Procedure

Step 1 Click **VoiceMail Mgt**. on the Manage Location page.

The screen shown in Figure C-30 appears.

Figure C-30 VoiceMail Management



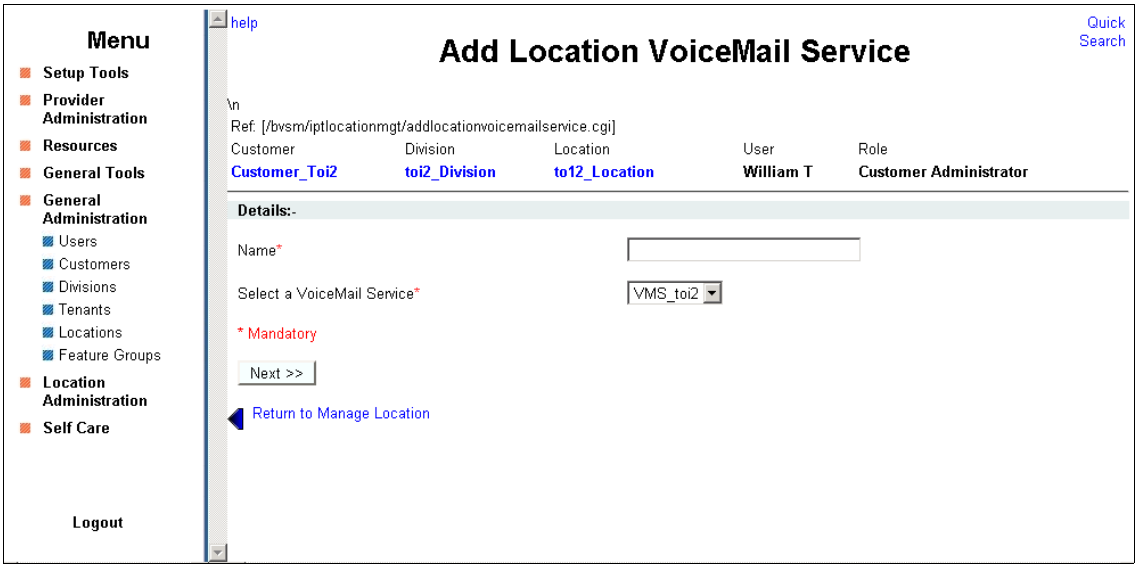
This page displays a list of the voicemail services in the current location. You can use this page to search for voicemail services in the database, to manage a specific voicemail service, or add a voicemail service.

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**.

The screen shown in Figure C-31 appears.

Figure C-31 Add Location VoiceMail Service



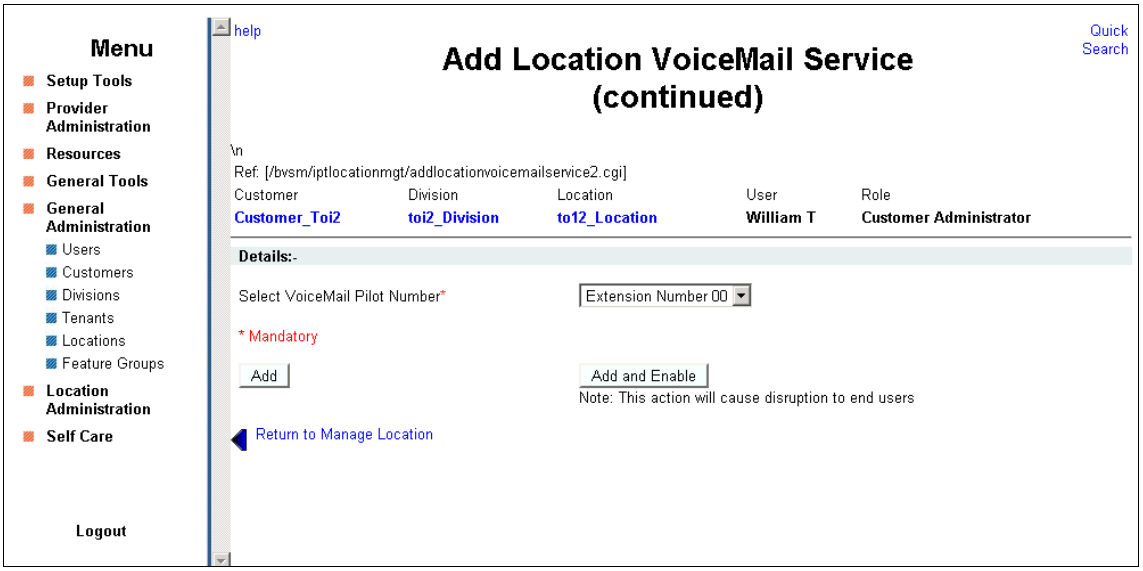
Step 4 Enter the voicemail service name.

Step 5 Select the voicemail resource from the pull-down selection list.

Step 6 Click **Next**.

The screen shown in Figure C-32 appears.

Figure C-32 Add Location VoiceMail Service (continued)



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 / configured at this location.

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.

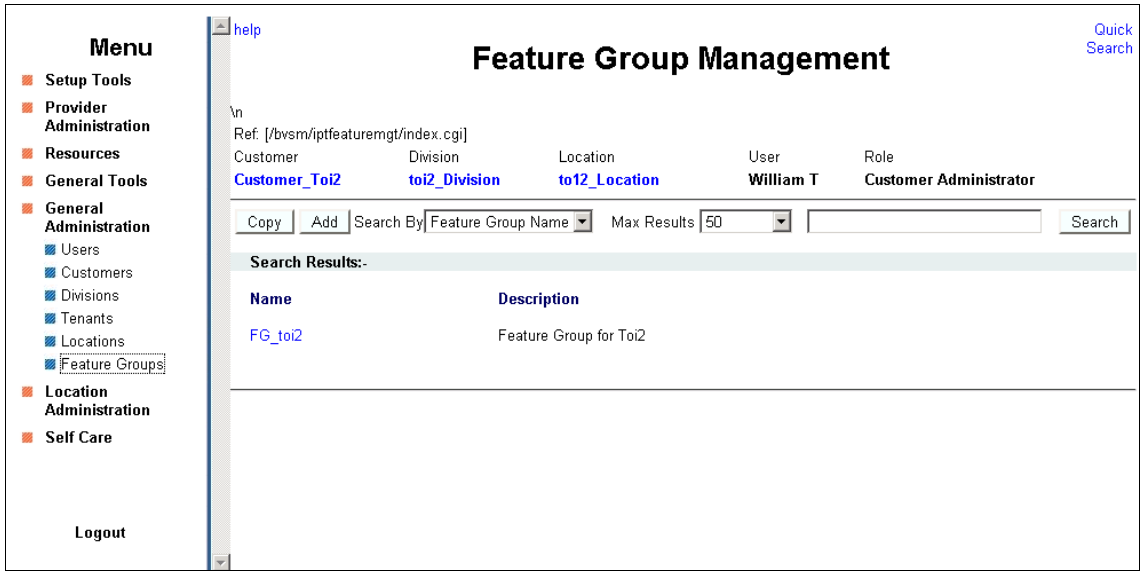
To manage feature groups, complete the following steps:

Procedure

Step 1 Select **Feature Groups** on the Location Administration menu.

The screen shown in Figure C-33 appears.

Figure C-33 Feature Group Management



This page displays a list of the feature groups in the Hosted UCS system. 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**.

The screen shown in Figure C-34 appears when you select an existing feature group.

Figure C-34 Manage Feature Group

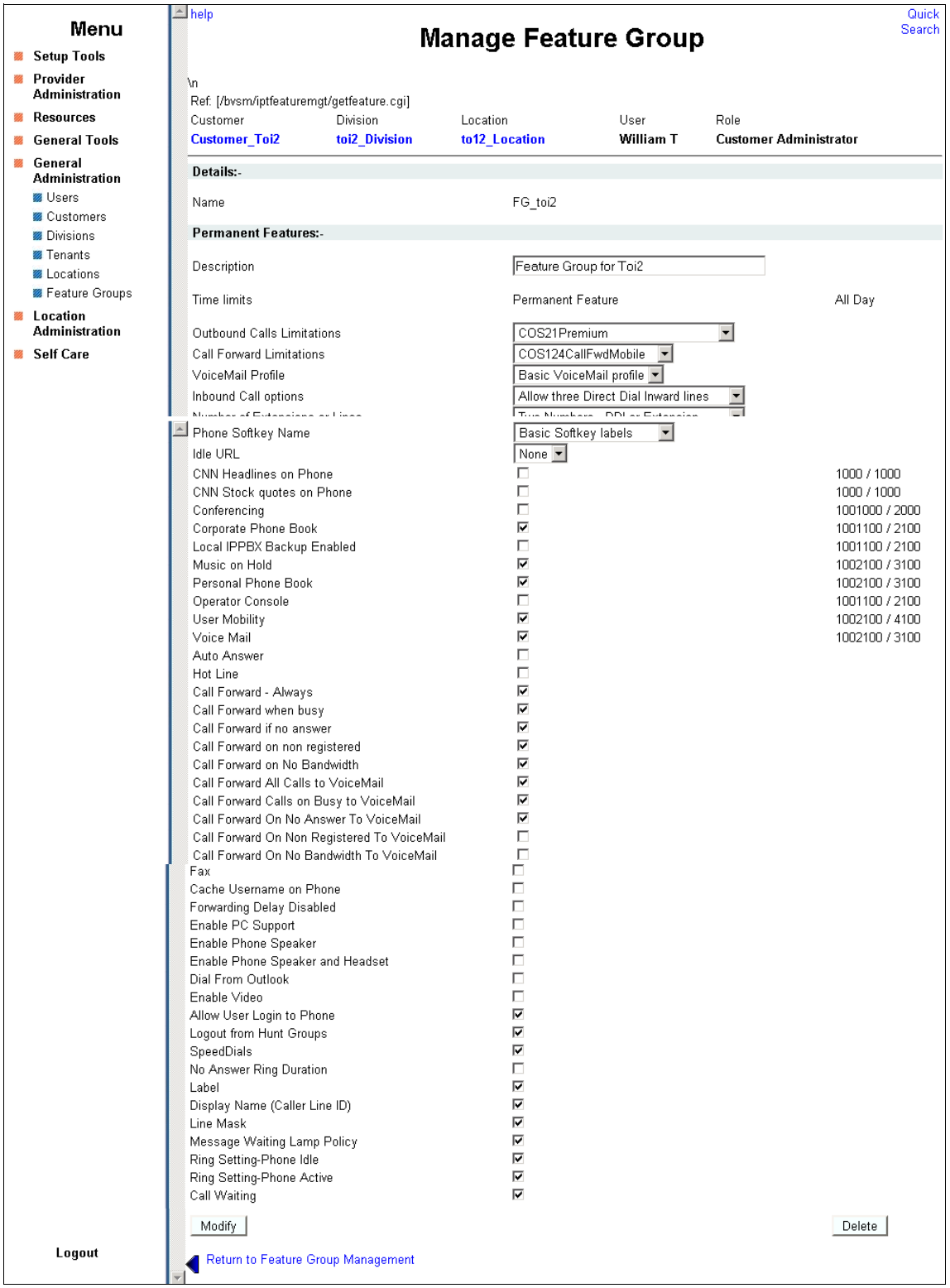


Figure C-34 lists the available feature groups.

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-40
- Telephony, page C-42
- Hunt Groups, page C-44
- Number Groups, page C-47
- Voicemail Groups, page C-48
- Pickup Groups, page C-49
- Users, page C-50
- Phone Inventory, page C-53
- Phone Registration, page C-54
- Phone Management, page C-55
- Analogue Line Reg., page C-56
- Analogue Line Mgt., page C-56
- MoH Track Mgt Option, page C-57
- Internal Numbers, page C-59
- External Numbers, page C-60
- Data Services, page C-62

Switchboards

Use the **Switchboards** option on the Location Administration menu to manage existing switchboards or to create a new switchboard.

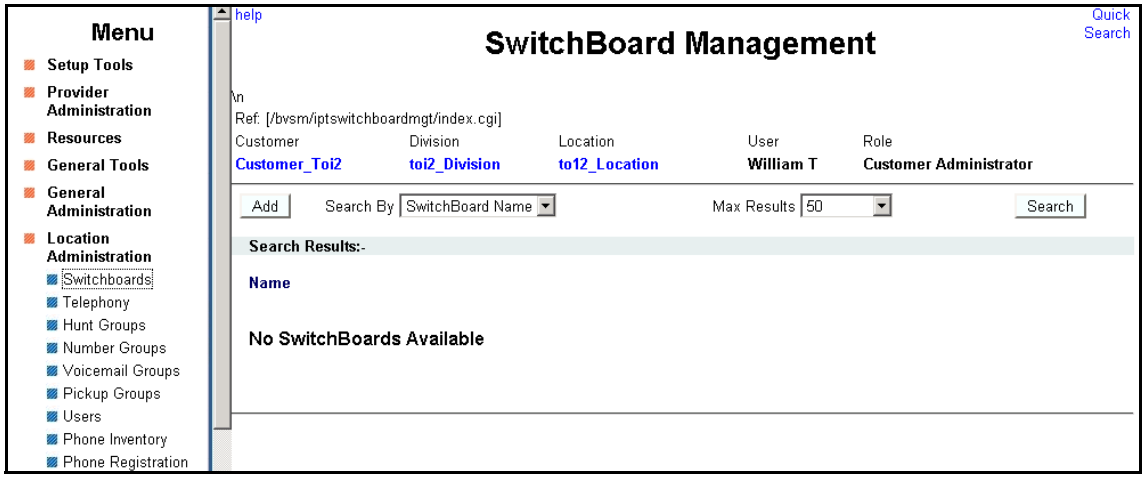
To manage switchboards, complete the following steps:

Procedure

Step 1 Select **Switchboards** on the Location Administration Menu.

The screen shown in Figure C-35 appears.

Figure C-35 SwitchBoard Management



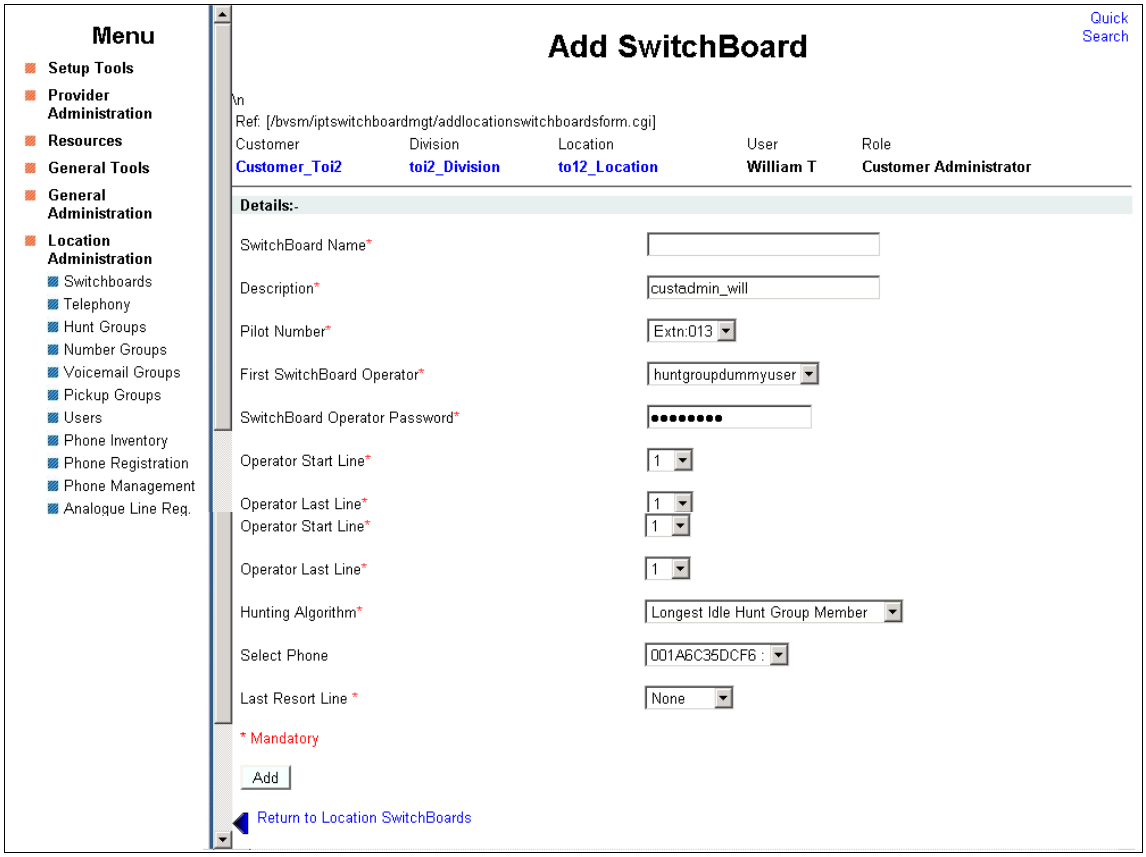
This page displays a list of the switchboards in the current location. You can use this page to search for switchboards in the database, to manage a specific switchboard, or add a switchboard.

Step 2 To manage an existing switchboard, click the blue link in the Name column.

Step 3 To add a switchboard, click **Add**.

The screen shown in Figure C-36 appears.

Figure C-36 Add Switchboard



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.

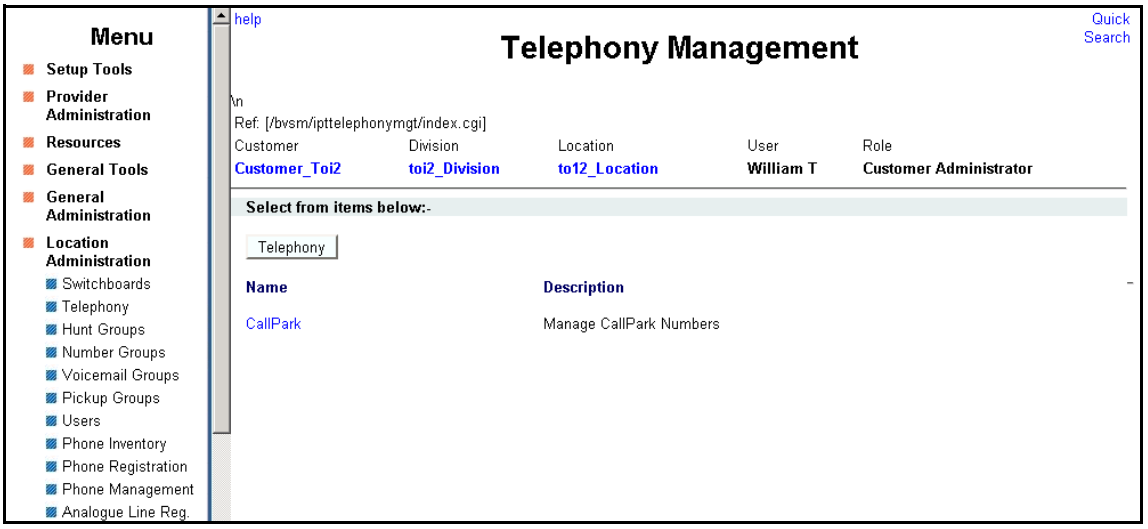
To manage telephony services for the location, complete the following steps:

Procedure

Step 1 Click the **Telephony** option on the Location Administration menu.

When you select the **Telephony** option**,** the screen shown in Figure C-37 appears.

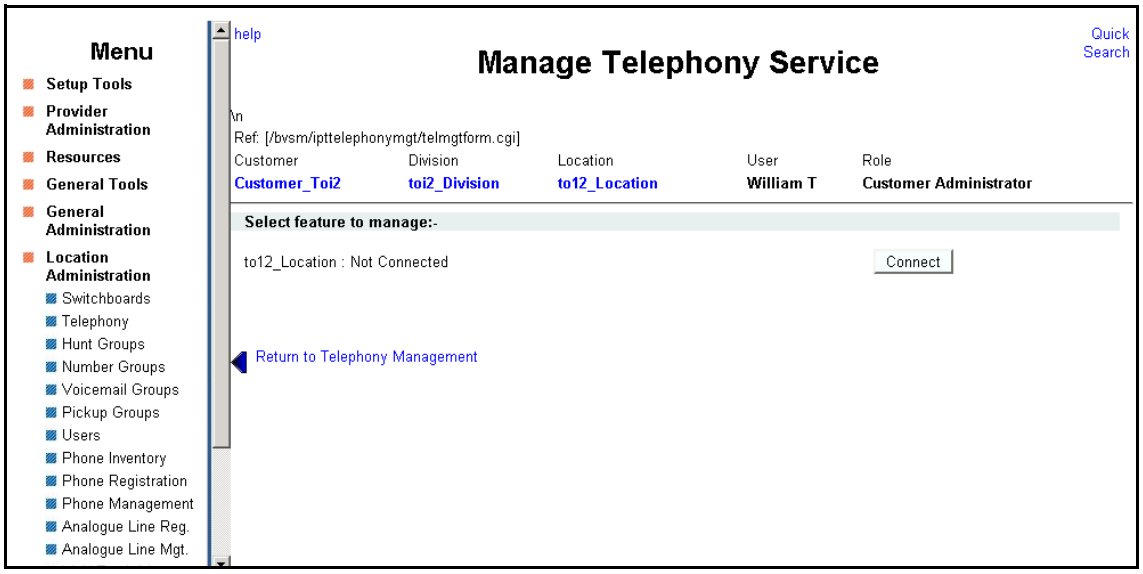
Figure C-37 Telephony Management



Step 2 To manage the telephony services click **Telephony**.

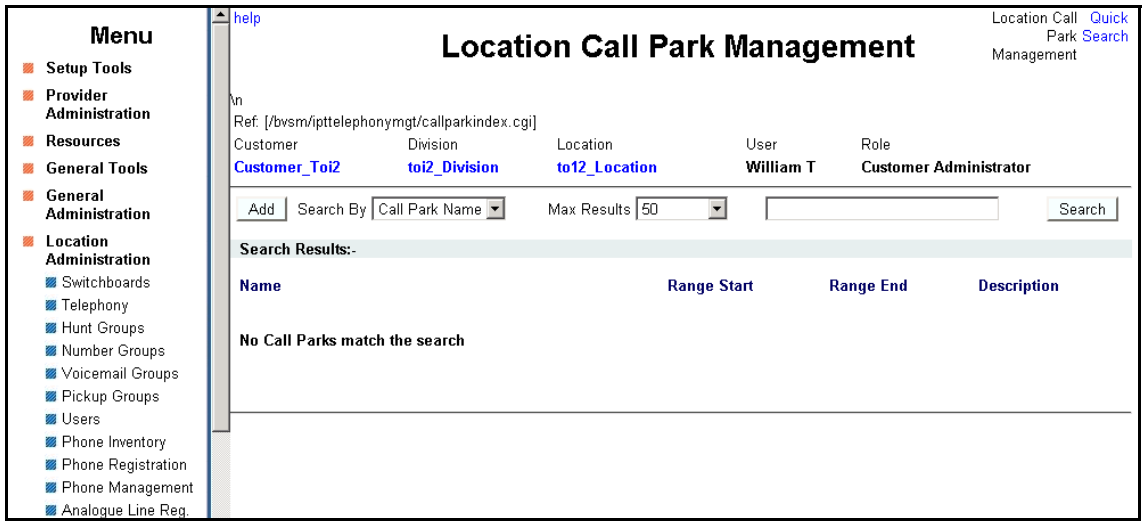
The screen shown in Figure C-38 appears.

Figure C-38 Manage Telephony Service



Step 3 To connect the telephony service, click **Connect**.

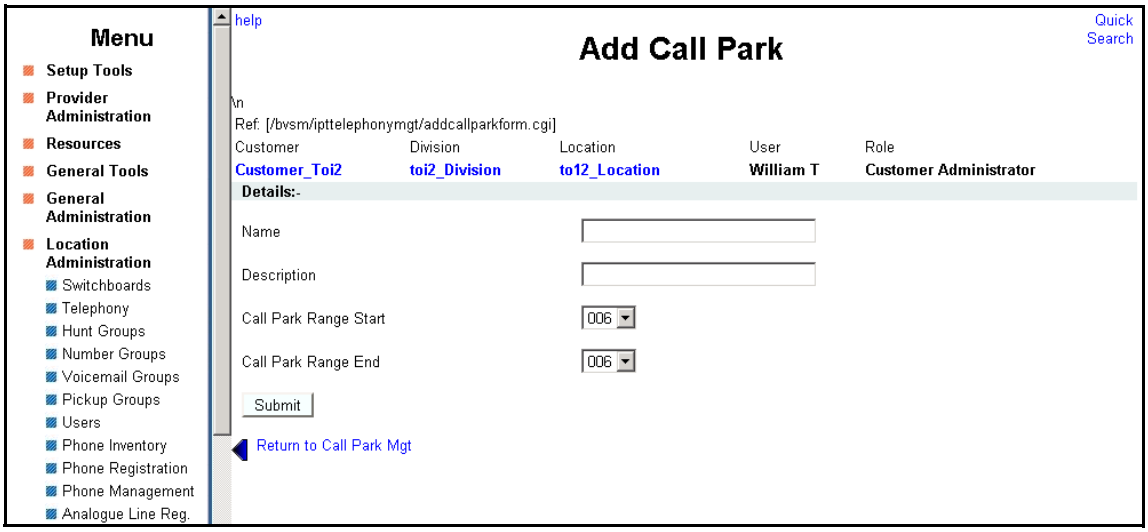
Figure C-39 To manage the Call Park Telephony service for the current location, click the blue link in the Name column.The screen shown in Figure C-39 appears.***Location Call Park Management***



To add a Call Park service, click **Add**.

The screen shown in Figure C-40 appears.

Figure C-40 Add Call Park



Step 4 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-47. 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."

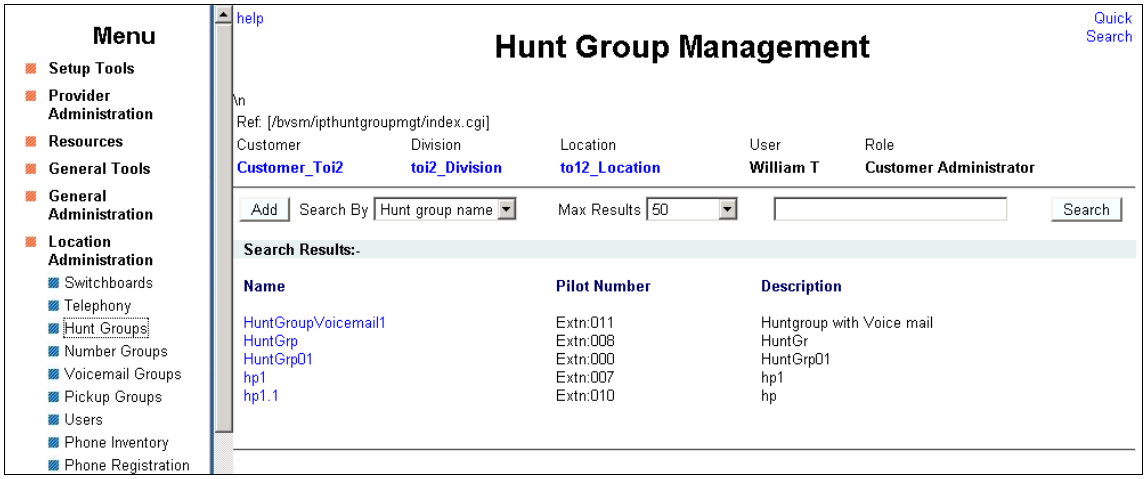
To create a hunt group, complete the following steps:

Procedure

Step 1 Select **Hunt Groups** on the Location Administration menu.

The Hunt Group Management page appears (see Figure C-41).

Figure C-41 Hunt Group Management

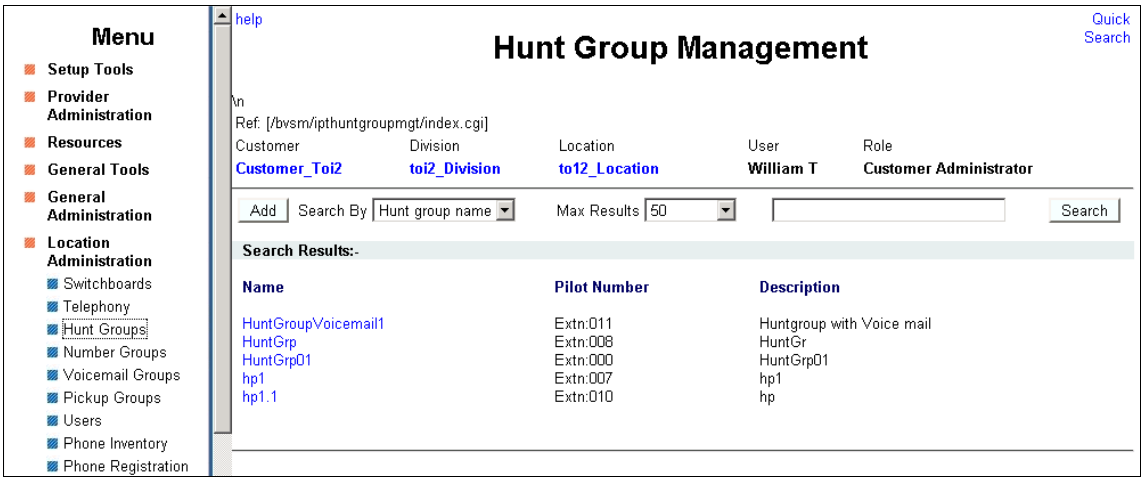


To search for a hunt group, select Hunt group name or description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add**.

The page shown in Figure C-42 appears.

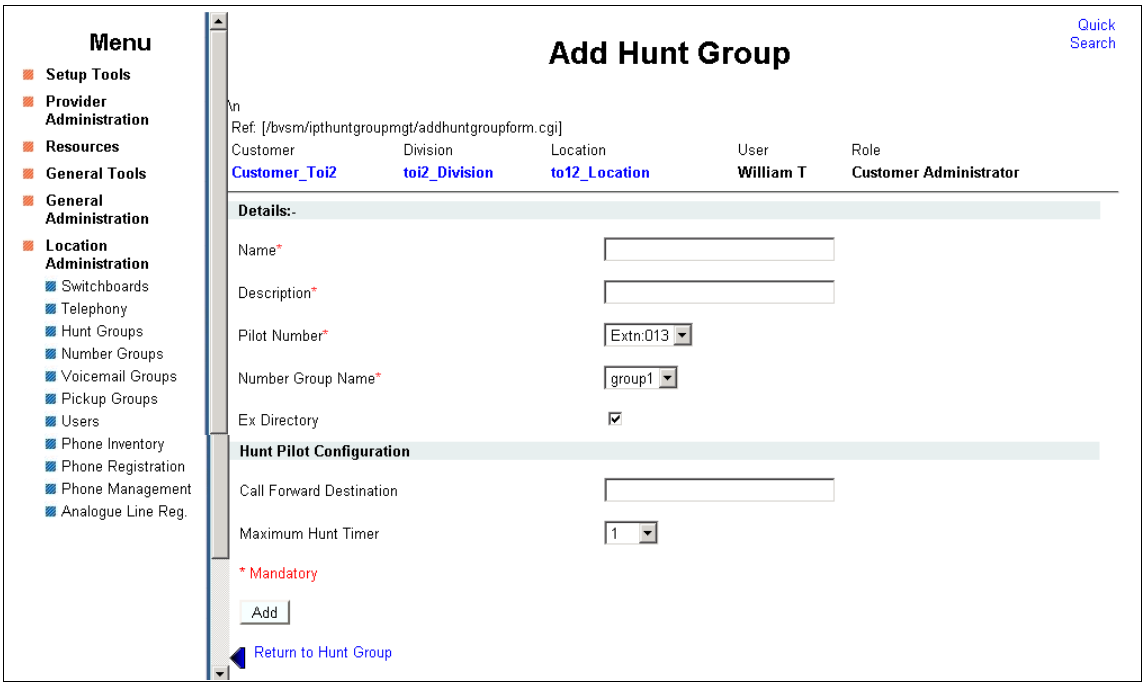
Figure C-42 Hunt Group Management



Step 3 Click **Add** to add a new hunt group.

The page shown in Figure C-43 appears.

Figure C-43 Add Hunt Group



Step 4 Enter a unique name for the hunt group.

Step 5 (Optional) Enter a description for the hunt group.

Step 6 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 7 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 8 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 9 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.

Voicemail Groups

Once a voicemail resource has been created for a customer, it can be allocated to a location by creating a voicemail service within the location. Once a voicemail service exists within a location, then user accounts can be created using an associated phone or Mobility profile). Once the user account is created, the user can manage their own voicemail account through the Self Service menu.

A voice mail group is a special voicemail account that is shared by a group of users. Use the **VoiceMail Groups** option on the Location Administration menu to manage existing voicemail group or to create a new voicemail group.

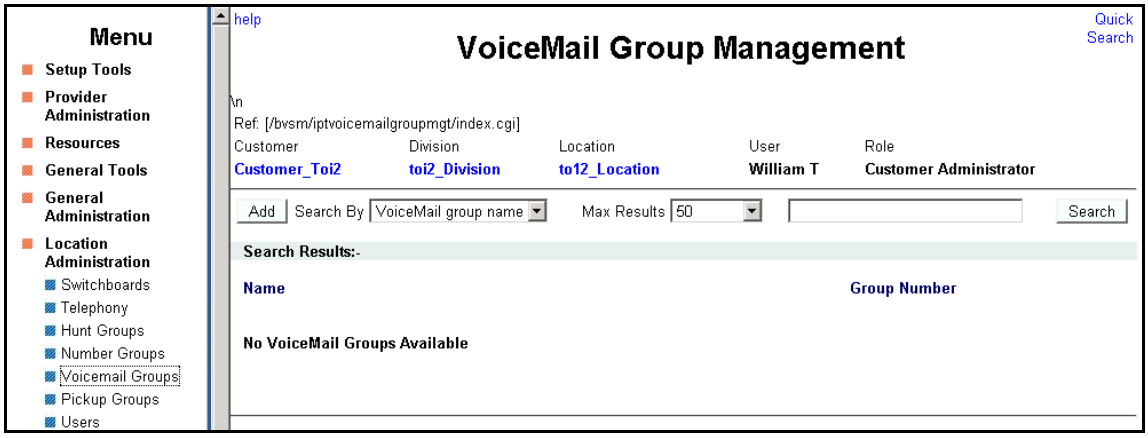
To manage voicemail groups, complete the following steps:

Procedure

Step 1 Select **VoiceMail Groups** on the Location Administration Menu.

The screen shown in Figure C-44 appears.

Figure C-44 VoiceMail Group Management



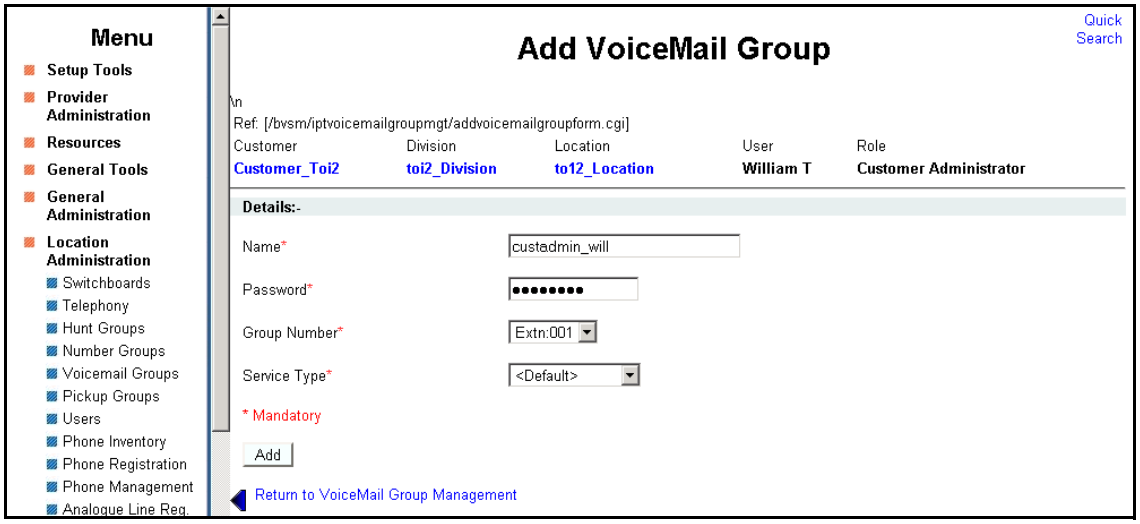
This page displays a list of the voicemail groups in the current location. You can use this page to search for voicemail groups in the database, to manage a specific voicemail group, or add a voicemail group.

Step 2 To manage an existing voicemail group, click the blue link in the Name column.

Step 3 To add a voicemail group, click **Add**.

The screen shown in Figure C-45 appears.

Figure C-45 Add VoiceMail Group



Step 4 Enter the information required for the voicemail group.

Step 5 Select the options required to configure the voicemail group from the pull-down selection lists.

Step 6 Click **Add**.

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.”

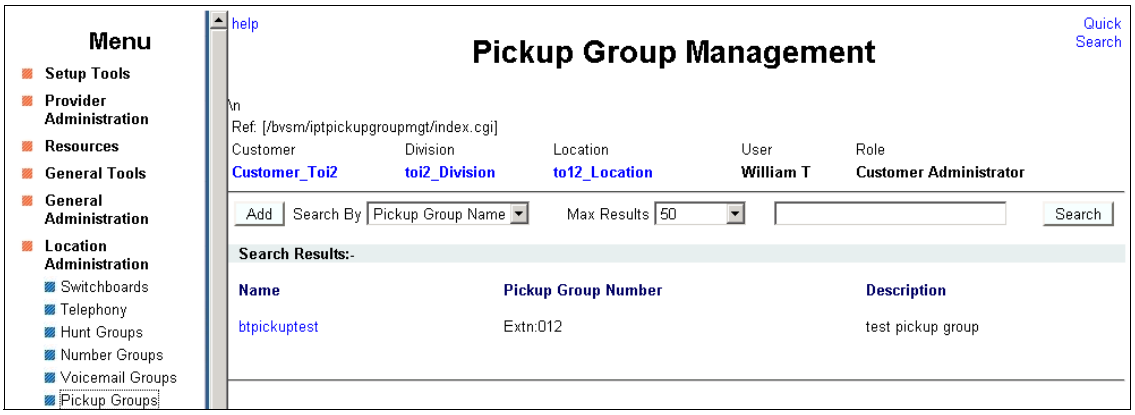
To create a pickup group, complete the following steps:

Procedure

Step 1 On the Location Administration menu, select **Pickup Groups**.

The Pickup Group Management page appears (see Figure C-46).

Figure C-46 Pickup Group Management

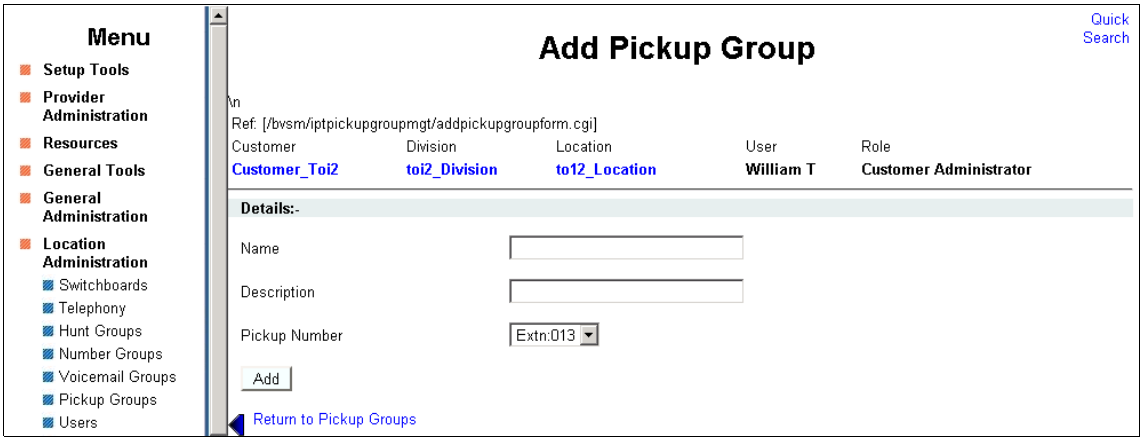


To search for a pickup group, select Pickup Group Name or Description from the Search by pull-down selection list, and type as many characters as you know in the field provided and click **Search**. The search string is case-sensitive.

Step 2 Click **Add** on the Pickup Group Management page.

The Add Pickup Group page appears (see Figure C-47).

Figure C-47 Add Pickup Group



Step 3 Enter a unique name for the pickup group.

Step 4 (Optional) Enter a description for the pickup group.

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.”

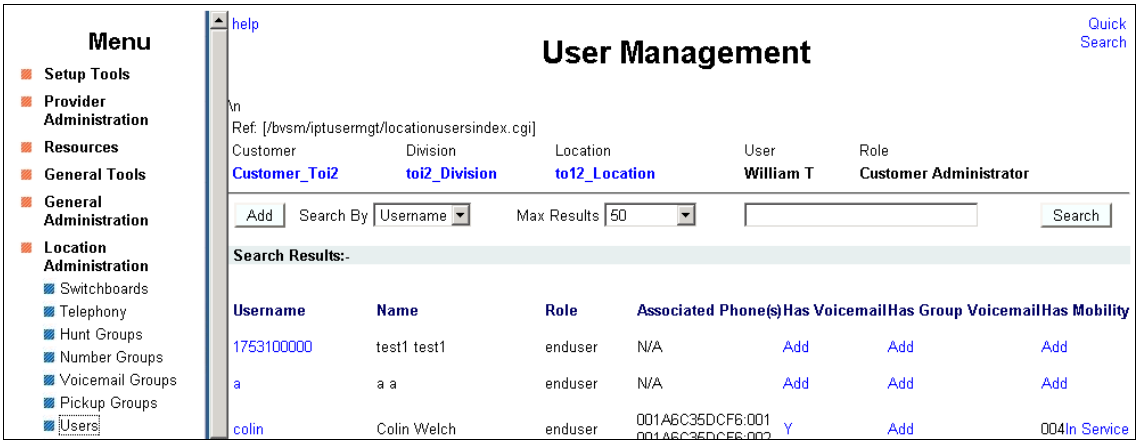
To change the permissions for a user, complete the following steps:

Procedure

Step 1 Click **User Management** on the Location Administration menu.

The screen shown in Figure C-48 appears.

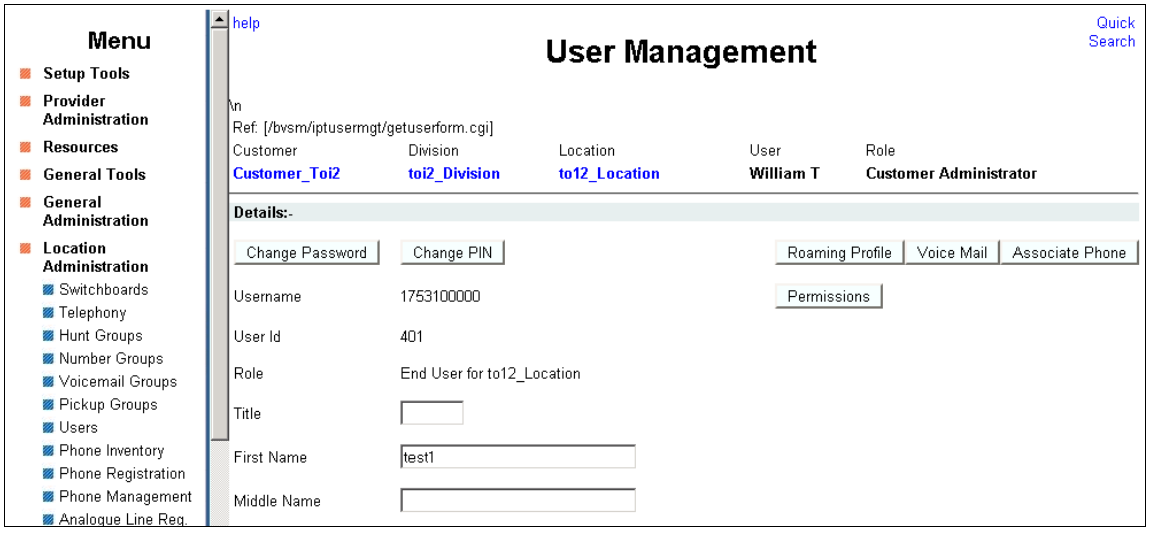
Figure C-48 Location/User Management



Step 2 Click the blue link in the Username column for the user account you want to manage.

The screen shown in Figure C-49 appears.

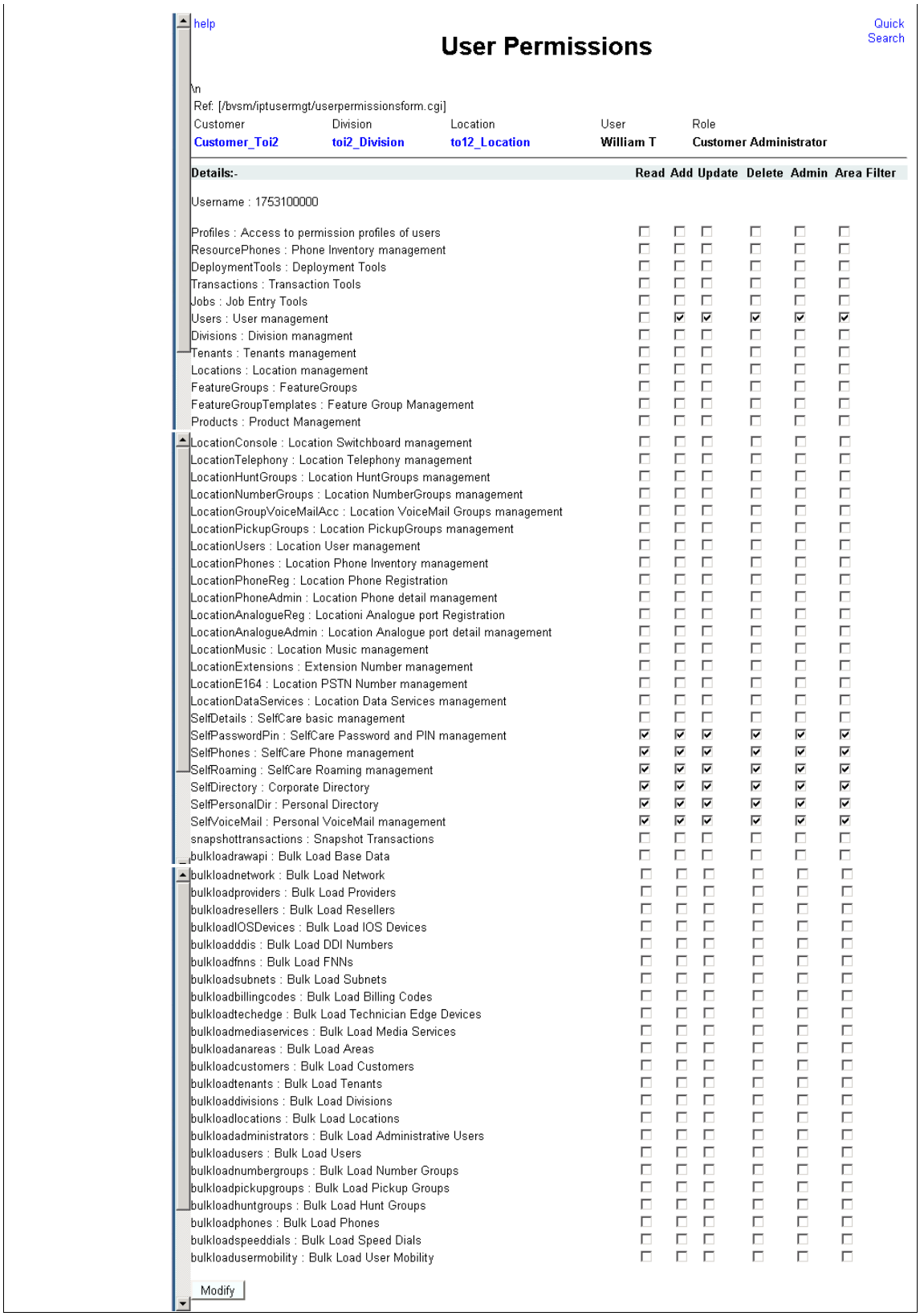
Figure C-49 Location/User Management—Page 2



Step 3 Click **Permissions**.

The screen shown in Figure C-50 appears.

Figure C-50 User 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.

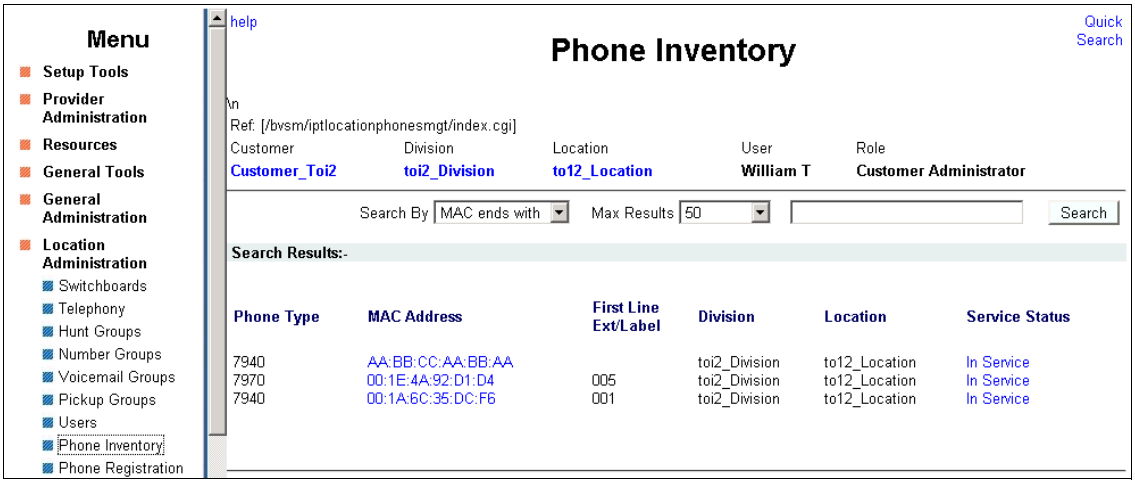
To manage the phone inventory, complete the following steps:

Procedure

Step 1 Select **Phone Inventory** on the General Administration Menu.

The screen shown in Figure C-51 appears.

Figure C-51 Phone Inventory



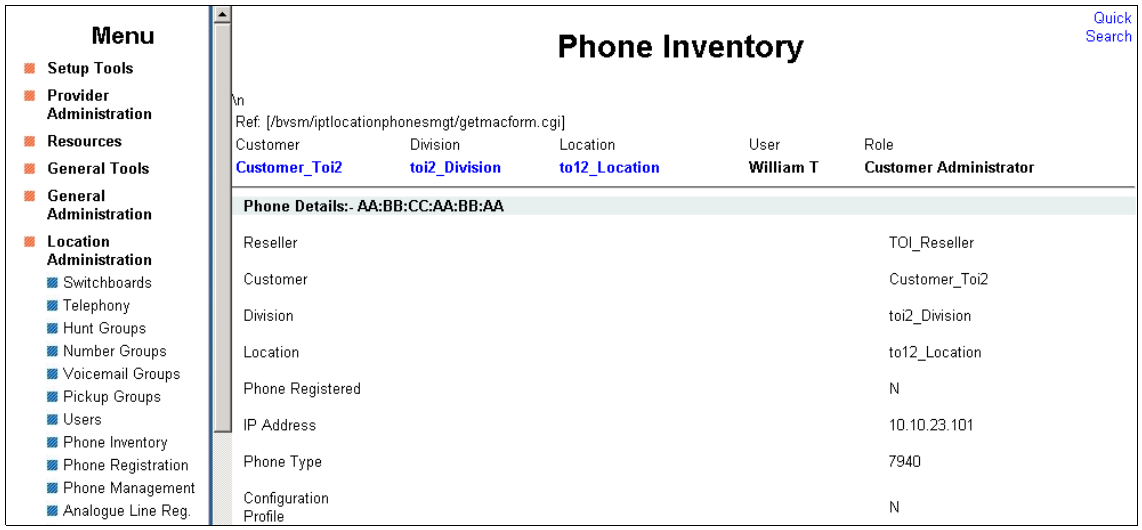
This page displays a list of the phone inventory in the current location. You can use this page to search for phones in the database and to manage a specific phone.

Step 2 To manage a phone, click the blue link in the Name column.

Step 3 To add a voicemail account, click **Add**.

The screen shown in Figure C-52 appears.

Figure C-52 Phone Inventory—Phone Details



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 BVSM 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.

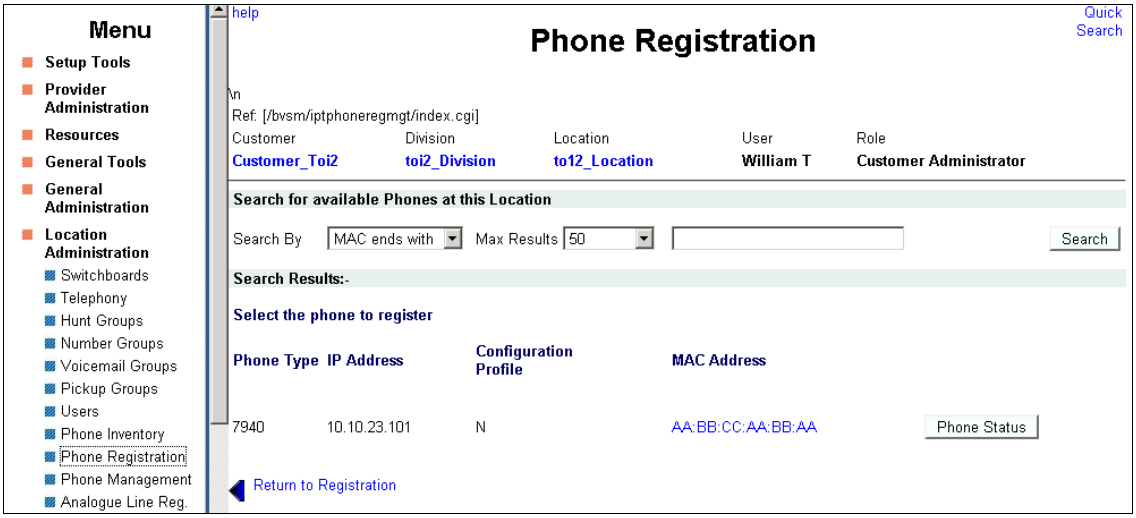
To register a phone, complete the following steps:

Procedure

Step 1 Select **Phone Registration** on the Location Administration Menu.

The screen shown in Figure C-53 appears.

Figure C-53 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.

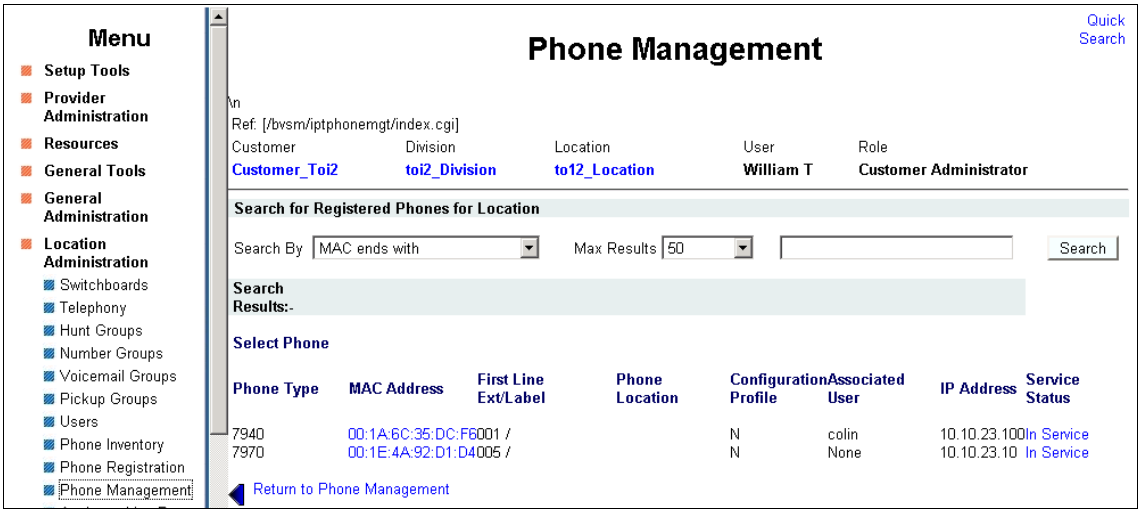
Step 2 To register a phone, click the blue link in the Name column.

For further information about registering phones, see Appendix A, "Location Administration."

Phone Management

Use the **Phone Management** option (Figure C-54) 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."

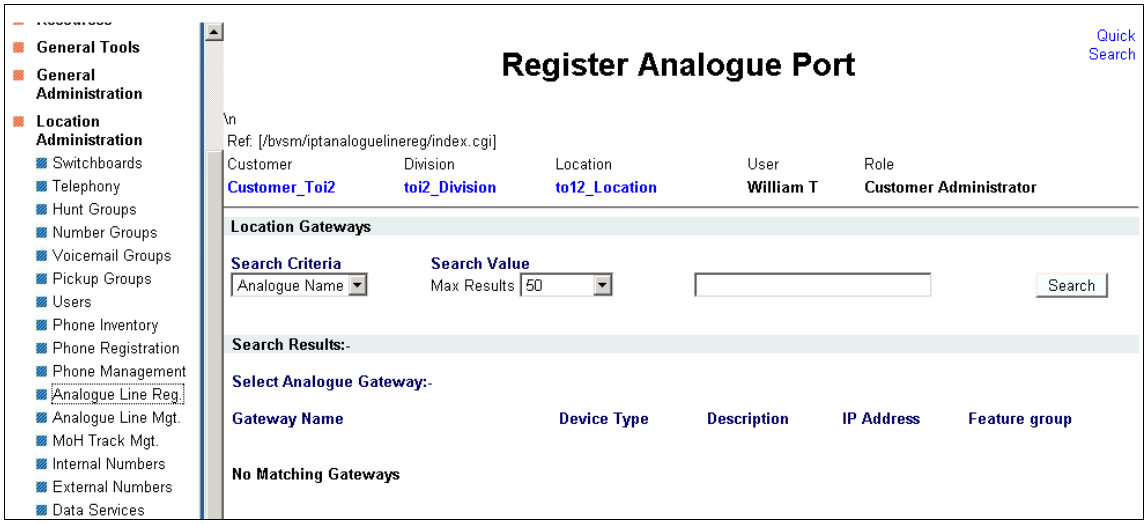
Figure C-54 Phone Management



Analogue Line Reg.

When you select the **Analogue Line Reg.** option, the screen shown in Figure C-55 appears.

Figure C-55 Register Analogue Port



This page displays a list of the unregistered analog ports in the current location. You can use this page to search for unregistered analog ports in the database, or to register an unregistered analog port.

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.

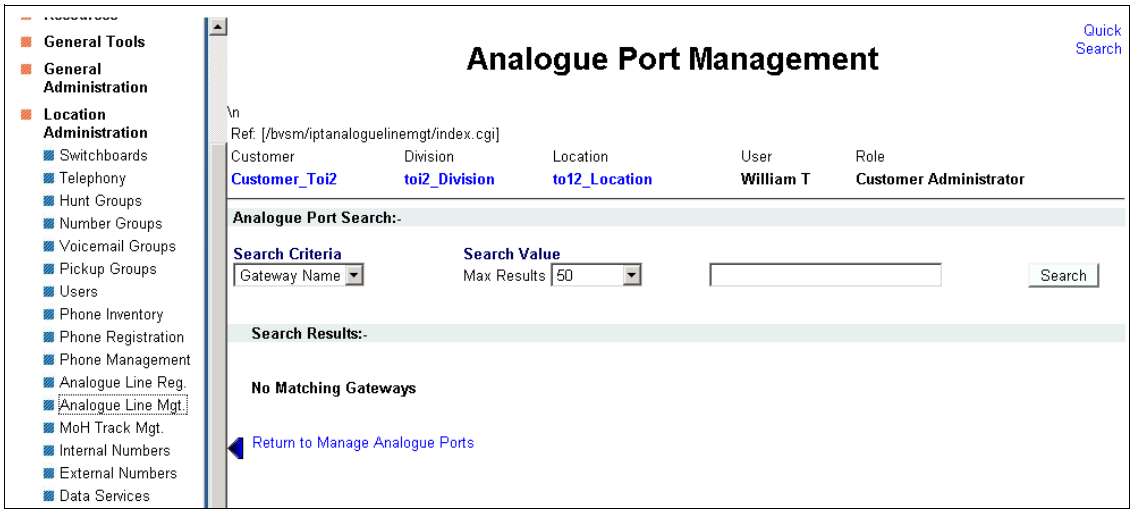
To register an analog line, complete the following steps:

Procedure

Step 1 Select **Analogue Line Mgt.** on the Location Administration menu.

The screen shown in Figure C-56 appears.

Figure C-56 Analogue Port Management



This page displays a list of the analogue in the current location. 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.

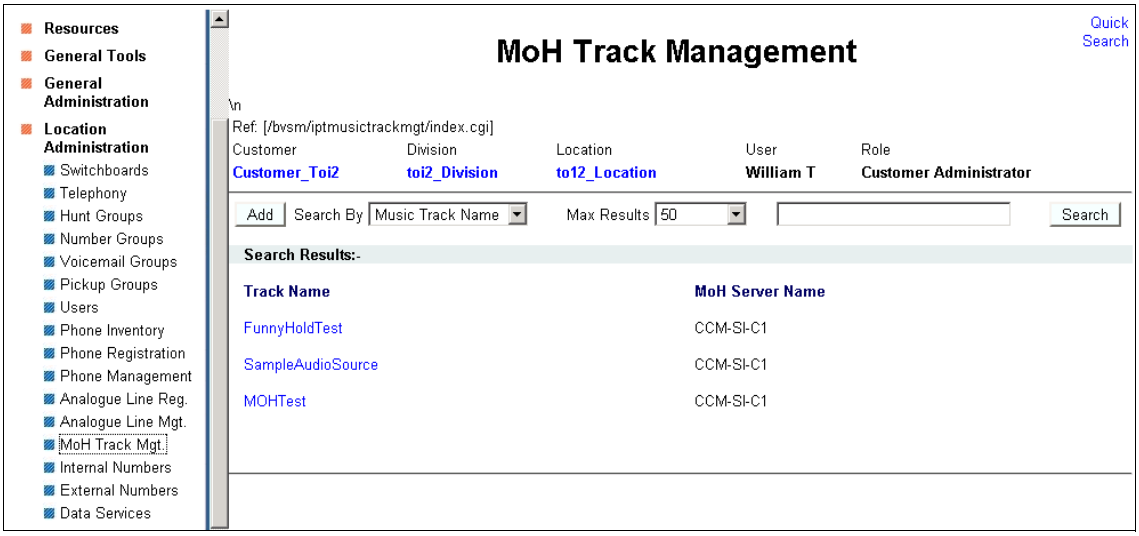
To manage MoH tracks, complete the following steps:

Procedure

Step 1 Select **MoH Track Mgt** on the Location Administration Menu.

The screen shown in Figure C-57 appears.

Figure C-57 MoH Track Management



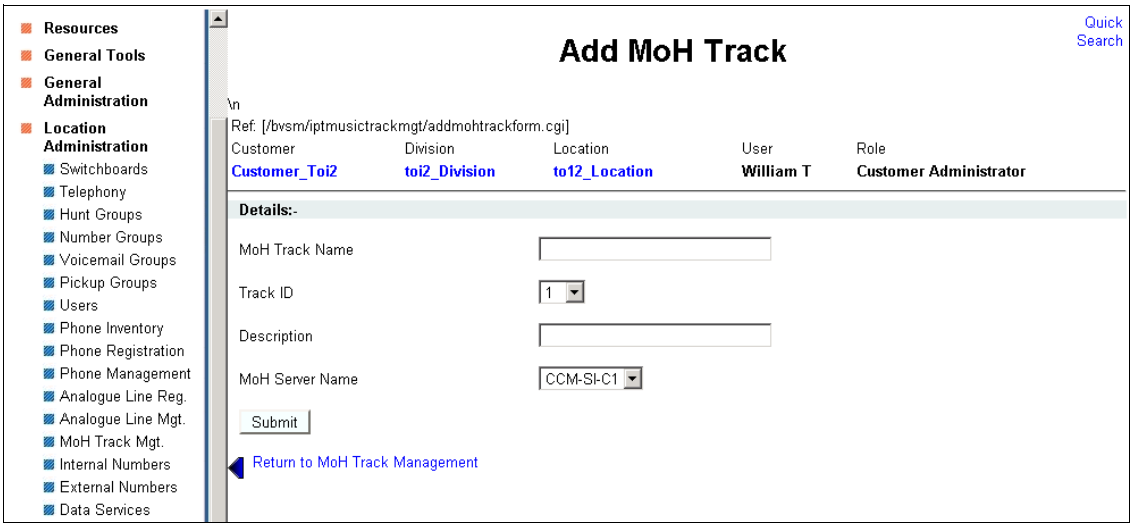
This page displays a list of the MoH tracks in the current location. You can use this page to search for MoH tracks in the database, to manage a specific MoH track, or add a MoH track.

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**.

The screen shown in Figure C-58 appears.

Figure C-58 Add MoH Track



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

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.

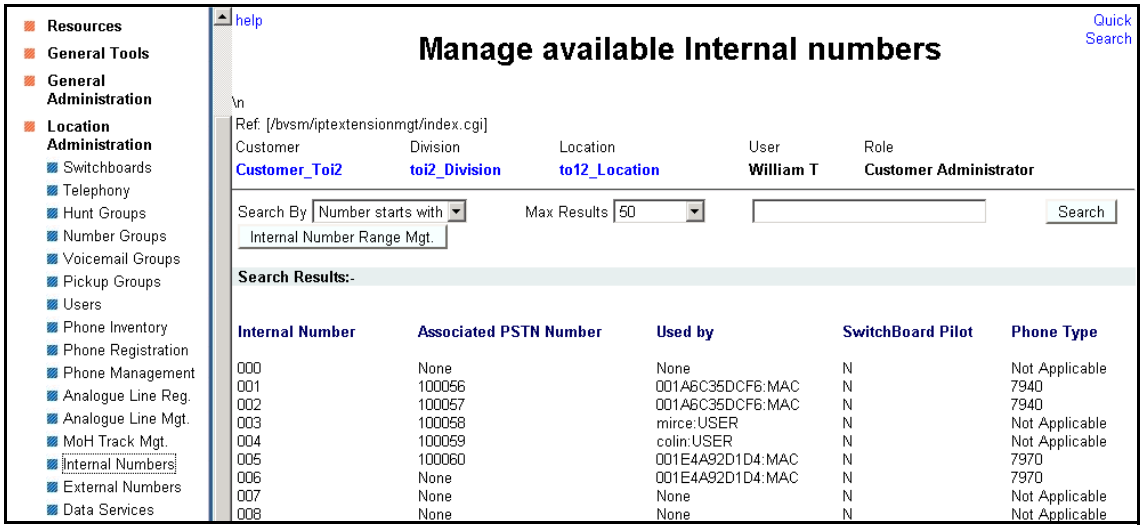
To manage internal numbers, complete the following steps:

Procedure

Step 1 Select **Internal Numbers** on the Location Administration Menu.

The screen shown in Figure C-59 appears.

Figure C-59 Manage available Internal numbers



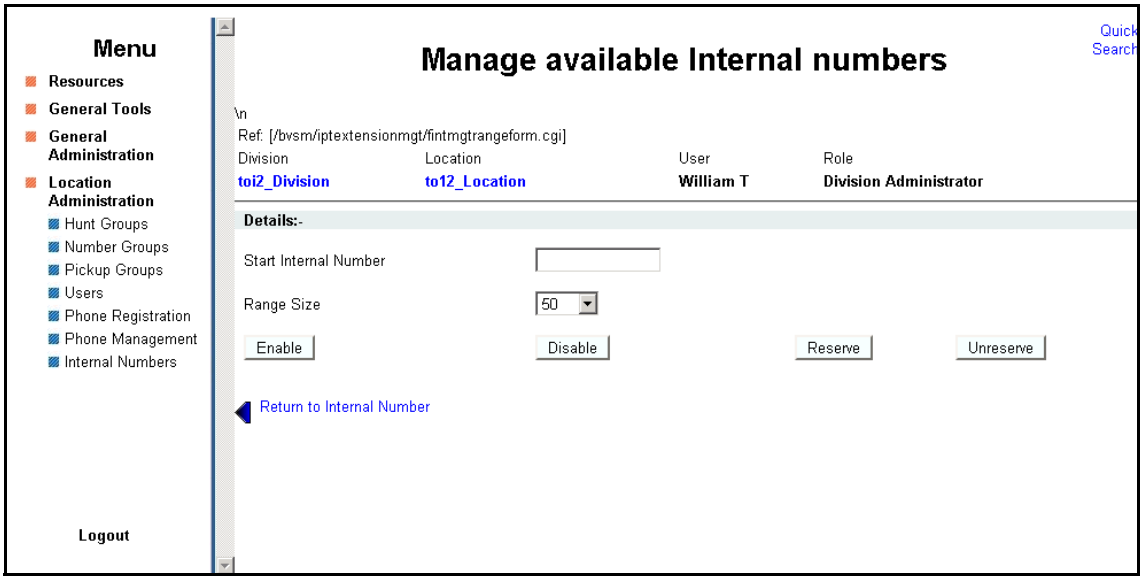
The Manage available internal numbers page provides a list of internal numbers, their associated PSTN numbers, their associated phone users, switchboard pilot, and type of phone. You can use this page to search for internal numbers in the database, or to manage the internal number range.

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.**

The screen shown in Figure C-60 appears.

Figure C-60 Internal Number Range Management



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.

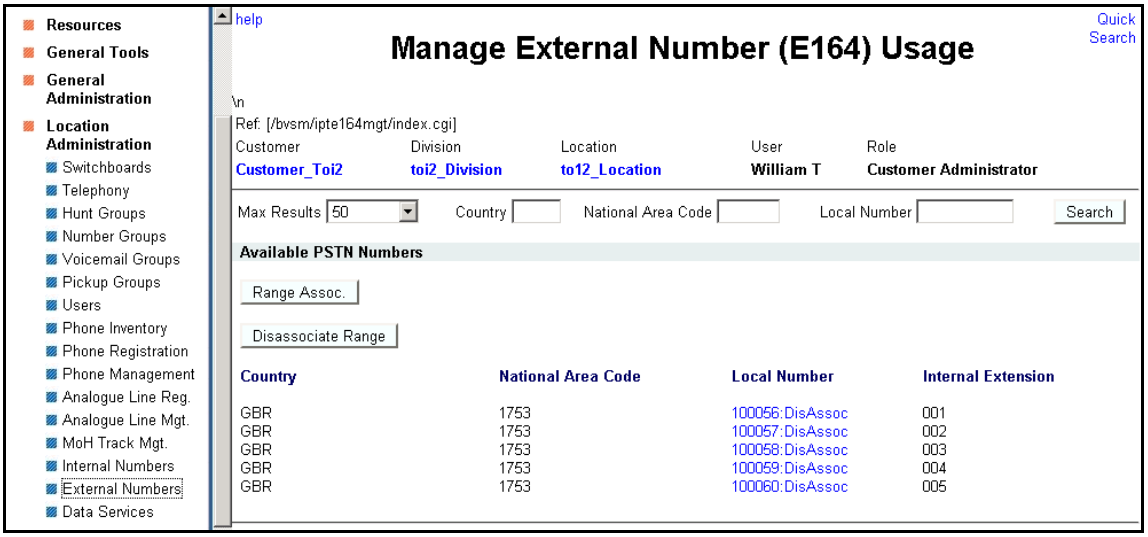
To manage external numbers, complete the following steps:

Procedure

Step 1 Select **External Numbers** on the Location Administration Menu.

The screen shown in Figure C-61 appears.

Figure C-61 Manage External Number (E164) Usage



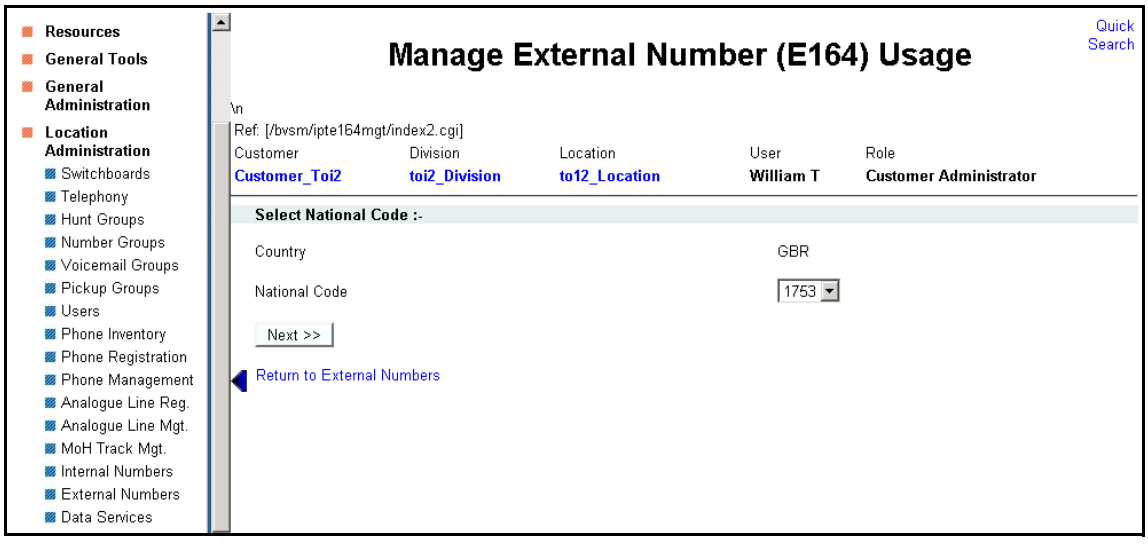
The Manage External Numbers Usage page lets you review the association between DDI and Internal numbers for you location, as well as removing the association for certain numbers. To disassociate numbers click **DisAssoc** next to the relevant DDI number.

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.**

The screen shown in Figure C-62 appears.

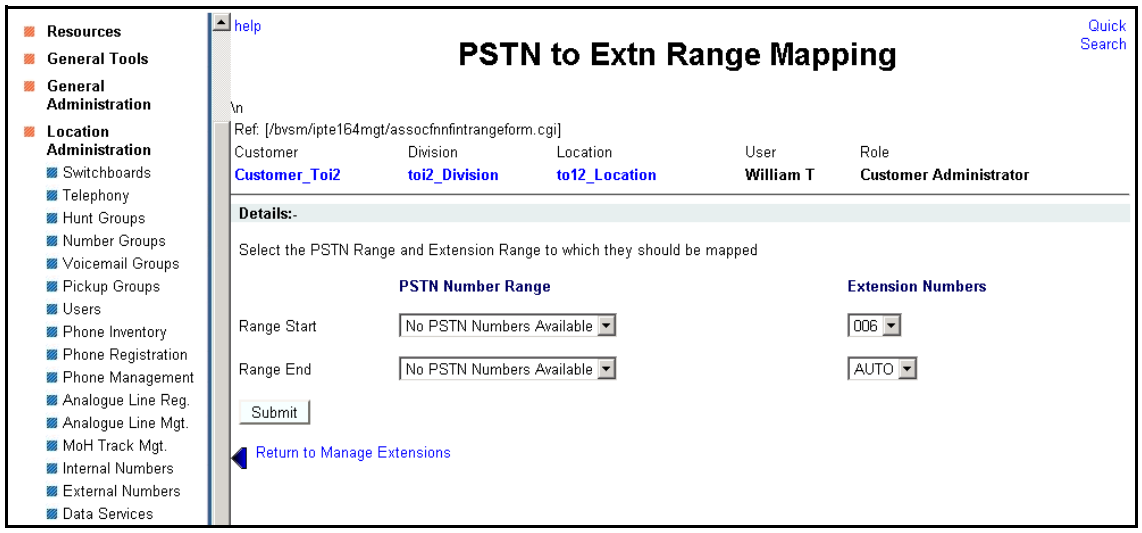
Figure C-62 Manage External Number (E165) Usage



Step 3 Select the national Code from the pull-down selection list.

The screen shown in Figure C-63 appears.

Figure C-63 PSTN to Extn Range Mapping



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**.

Data Services

Use the **Data Services** option on the Location Administration menu to manage LAN switches in the location.

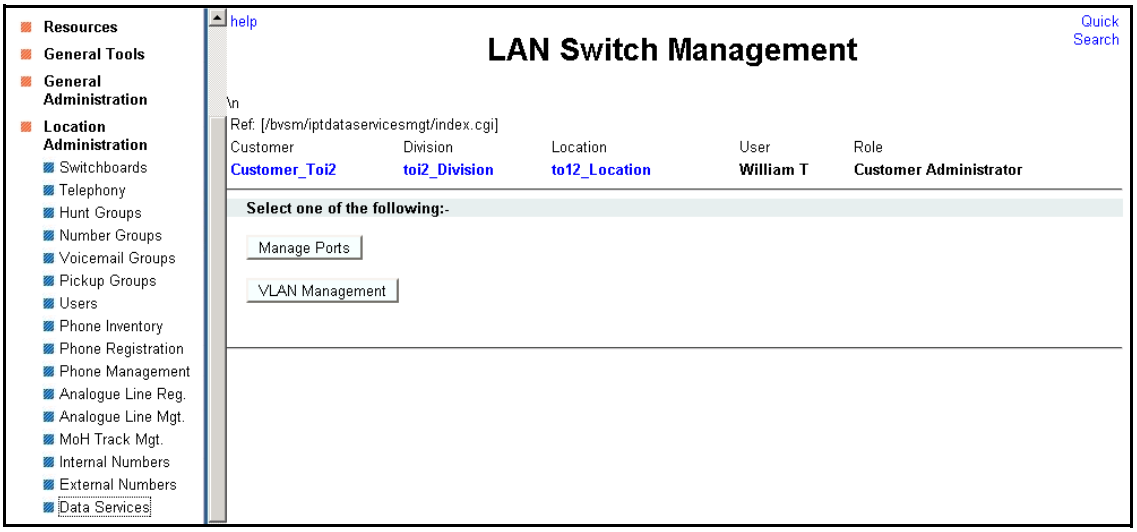
To manage LAN switches, complete the following steps:

Procedure

Step 1 Select **Data Services** on the Location Administration Menu.

The screen shown in Figure C-64 appears.

Figure C-64 LAN Switch Management



This page displays a list of the LAN switches in the current location. You can use this page to manage ports or VLANs.

Step 2 To manage ports, click **Manage Ports**.

Step 3 To manage VLANs, click **VLAN Management**.