Cisco Unified Communications Manager
Features and Services Guide for Cisco Unified Communications Manager

Release 8.5(1)
CONTENTS

Preface xxxvii

CHAPTER 1

Barge and Privacy 1-1
  Configuration Checklists for Barge 1-2
  Configuration Checklist for Privacy and Privacy on Hold 1-4
  Introducing Barge, Privacy, and Privacy on Hold 1-5
    Barge 1-6
    Single Button Barge/cBarge 1-6
      Barge Using Built In Conference—Single Button Barge or Barge Softkey 1-8
      Barge by Using Shared Conference—Single Button cBarge or cBarge Softkey 1-9
      Barge Phone Display Messages 1-9
      Party Entrance Tone and Barge, cBarge, or Single Button Barge 1-9
    Privacy 1-10
    Privacy on Hold 1-10
  System Requirements for Barge, Privacy, and Privacy on Hold 1-11
  Devices That Support Barge and Privacy 1-11
  Interactions and Restrictions 1-12
    Interactions 1-13
      Barge and cBarge 1-13
      Barge and Call Park 1-13
      Barge and Join 1-13
      Barge, cBarge, and Single Button Barge Support for PLAR 1-13
    Restrictions 1-14
  Installing and Activating Barge, Privacy, and Privacy on Hold 1-16
    Activating Barge with Built In Conference Bridge 1-16
    Activating cBarge with Shared Conference Bridge 1-16
    Activating Privacy 1-16
    Activating Privacy on Hold 1-16
  Configuring Barge, Privacy, and Privacy on Hold 1-17
    Setting the Service Parameters for Barge, Privacy, and Privacy on Hold 1-17
  Related Topics 1-17

CHAPTER 2

Call Back 2-1
  Configuration Checklist for Call Back 2-1
Introducing Call Back  2-3
Understanding How Call Back Works  2-3
Suspend/Resume Functionality for Call Back  2-5
System Requirements for Call Back  2-6
Interactions and Restrictions  2-7
  Additional Information on Call Back Notification with Phones That Are Running SIP  2-8
  Feature Interactions with Call Forward, iDivert, and Voice-Messaging System Features  2-8
Installing and Activating Call Back  2-9
Configuring Call Back Softkey  2-9
  Creating a Softkey Template for the CallBack Softkey  2-9
  Configuring CallBack Softkey Template in Common Device Configuration  2-10
  Adding CallBack Softkey Template in Phone Configuration  2-11
Configuring Call Back Feature Button  2-11
  Creating a Phone Button Template for the CallBack Feature Button  2-11
  Adding CallBack Phone Button Template in Phone Configuration  2-12
  Setting Call Back Service Parameters  2-12
Providing Call Back Information to Users  2-13
Troubleshooting Call Back  2-13
Related Topics  2-13

CHAPTER 3

Call Control Discovery  3-1
Configuration Checklist for Call Control Discovery  3-2
Introducing Call Control Discovery for Cisco Unified Communications Manager  3-5
  Overview of Call Control Discovery  3-5
  Components for the Call Control Discovery Feature  3-6
    Call Control Discovery Terminology  3-6
    Call Control Discovery Advertising Service  3-8
    Call Control Discovery Requesting Service  3-10
    SAF Forwarders  3-13
System Requirements for Call Control Discovery  3-16
Interactions and Restrictions  3-16
Installing and Activating Call Control Discovery  3-18
Configuring Call Control Discovery  3-18
  Considerations for Call Control Discovery Configuration  3-19
  Call Control Discovery Feature Parameters  3-23
  SAF Security Profile Configuration Settings  3-25
  SAF Forwarder Configuration Settings  3-26
  Hosted DN Group Configuration Settings  3-31
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted DN Pattern Configuration Settings</td>
<td>3-32</td>
</tr>
<tr>
<td>CCD Advertising Service Configuration Settings</td>
<td>3-34</td>
</tr>
<tr>
<td>Partition Configuration Settings for Call Control Discovery</td>
<td>3-36</td>
</tr>
<tr>
<td>CCD Requesting Service Configuration Settings</td>
<td>3-37</td>
</tr>
<tr>
<td>Blocked Learned Pattern Configuration Settings</td>
<td>3-40</td>
</tr>
<tr>
<td>Finding Configuration Records for Call Control Discovery</td>
<td>3-42</td>
</tr>
<tr>
<td>Configuring Call Control Discovery (Procedure)</td>
<td>3-44</td>
</tr>
<tr>
<td>Configuring a SAF-Enabled Trunk</td>
<td>3-45</td>
</tr>
<tr>
<td>Identifying Which Hosted DN Patterns Belong to a Hosted DN Group</td>
<td>3-46</td>
</tr>
<tr>
<td>Deleting Configuration Records for Call Control Discovery</td>
<td>3-46</td>
</tr>
<tr>
<td>Providing Information to End Users</td>
<td>3-47</td>
</tr>
<tr>
<td>Troubleshooting Call Control Discovery</td>
<td>3-47</td>
</tr>
<tr>
<td>Related Topics</td>
<td>3-47</td>
</tr>
</tbody>
</table>

## CHAPTER 4

### Call Display Restrictions 4-1

- Configuration Checklist for Call Display Restrictions 4-1
- Introducing Call Display Restrictions 4-2
  - Overview of Call Display Restrictions 4-3
  - Enabling Call Display Restrictions 4-3
- System Requirements for Call Display Restrictions 4-4
- Scenarios for Using Call Display Restrictions 4-4
- Interactions 4-5
  - Call Park 4-5
  - Conference List 4-6
  - Conference and Voice Mail 4-6
  - Extension Mobility 4-6
- Configuring Call Display Restrictions 4-6
  - Configuring the Translation Pattern Parameters 4-7
  - Configuring the Phone Configuration 4-8
- Sample Configurations 4-9
  - Partitions 4-9
  - Calling Search Spaces 4-10
  - Devices and Gateways 4-10
  - Translation Patterns 4-11
  - Call Park 4-13
- Sample Call Flow 4-13
- Setting the Service Parameter for Connected Number Display Restriction 4-14
- Related Topics 4-14
CHAPTER 5

**Call Park and Directed Call Park** 5-1

Call Park Configuration Checklist 5-2
Directed Call Park Configuration Checklist 5-3
Introducing Call Park 5-4
System Requirements for Call Park 5-7
Interactions and Restrictions 5-8

Interactions 5-8

CTI Applications 5-8
Music On Hold 5-9
Route Plan Report 5-9
Calling Search Space and Partitions 5-9
Immediate Divert 5-9
Barge 5-9
Directed Call Park 5-9
Q.SIG Intercluster Trunks 5-10

Restrictions 5-10

Installing and Activating Call Park 5-10
Configuring Call Park 5-11

Setting the Service Parameters for Call Park 5-11
Finding a Call Park Number 5-11
Configuring a Call Park Number 5-13
Call Park Configuration Settings 5-13
Deleting a Call Park Number 5-15

Park Monitoring for Cisco Unified IP Phones 8961, 9951, and 9971 5-16

Setting the Service Parameters for Park Monitoring 5-16
Setting Park Monitoring Parameters in Directory Number Configuration Window 5-18
Setting Park Monitoring Parameter in Hunt Pilot Configuration Window 5-18

Introducing Directed Call Park 5-19
System Requirements for Directed Call Park 5-20
Interactions and Restrictions 5-20

Interactions 5-20

Music On Hold 5-21
Route Plan Report 5-21
Calling Search Space and Partitions 5-21
Immediate Divert 5-21
Barge 5-21
Call Park 5-22

Restrictions 5-22
Installing and Activating Directed Call Park  5-23
Configuring Directed Call Park  5-23
  Setting the Service Parameters for Directed Call Park  5-23
  Finding a Directed Call Park Number  5-23
  Configuring a Directed Call Park Number  5-24
  Directed Call Park Configuration Settings  5-25
  Configuring BLF/Directed Call Park Buttons  5-27
  BLF/Directed Call Park Configuration Settings  5-27
  Synchronizing Directed Call Park With Affected Devices  5-28
  Deleting a Directed Call Park Number  5-29
Assisted Directed Call Park for Cisco Unified IP Phones (SIP)  5-29
Related Topics  5-30

CHAPTER  6
Call Pickup  6-1
  Configuration Checklist for Call Pickup and Group Call Pickup  6-1
  Configuration Checklist for Other Group Pickup  6-3
  Configuration Checklist for Directed Call Pickup  6-5
  Configuration Checklist for BLF Call Pickup  6-7
  Introducing Call Pickup  6-10
    Call Pickup  6-11
    Group Call Pickup  6-11
    Other Group Pickup  6-12
    Directed Call Pickup  6-12
      Examples of Directed Call Pickup  6-13
    Busy Lamp Field Call Pickup  6-16
      BLF Call Pickup Example  6-17
    Auto Call Pickup  6-17
      Call Pickup No Answer  6-18
      Call Pickup Busy  6-18
      Call Pickup No Bandwidth  6-18
    Using Call Pickup Features with Hunt Lists  6-19
    Using Call Pickup Features with Partitions to Restrict Access  6-21
    Call Pickup Notification  6-21
    System Requirements for Call Pickup  6-22
  Interactions and Restrictions  6-23
    Interactions  6-24
      Route Plan Report  6-24
      Calling Search Space and Partitions  6-24
      Time of Day  6-24

Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communications Manager
OL-22753-01
### Chapter 6: Call Accounting

- Dependency Records 6-25
- Restrictions 6-25
- Installing and Activating Call Pickup 6-25
- Configuring Call Pickup Features 6-26
  - Setting the Service Parameters for Call Pickup 6-26
- Configuring Call Pickup Groups 6-27
  - Finding a Call Pickup Group 6-27
  - Configuring a Call Pickup Group 6-28
  - Call Pickup Group Configuration Settings 6-29
- Deleting a Call Pickup Group 6-32
- Defining a Pickup Group for Other Group Pickup 6-33
- Assigning a Call Pickup Group to Directory Numbers 6-33
- Assigning a Call Pickup Group to Hunt Pilots 6-34

### Chapter 7: Call Throttling and the Code Yellow State

- Introducing Call Throttling 7-1
- Troubleshooting Call Throttling 7-2

### Chapter 8: Calling Party Normalization

- Configuration Checklist for Calling Party Normalization 8-1
- Introducing Calling Party Normalization 8-4
  - Globalizing the Calling Party Number 8-5
  - Localizing the Calling Party Number 8-7
  - Mapping the Global Party Calling Number to Its Local Variant 8-9
- System Requirements 8-10
- Interactions and Restrictions 8-10
  - Interactions 8-11
    - Globalizing and Localizing Calling Party Numbers for Transferred Calls 8-11
    - Globalizing and Localizing Calling Party Numbers for Forwarded Calls 8-11
    - Bulk Administration Tool 8-12
    - Call Detail Records 8-12
    - Cisco Unified Communications Manager Assistant 8-12
    - Cisco Unified Communications Manager CDR Analysis and Reporting 8-12
    - Cisco Unity/Cisco Unity Connection 8-12
    - Cisco Extension Mobility 8-13
Device Mobility 8-13
Restrictions 8-14
Installing and Activating Calling Party Normalization 8-15
Configuring Calling Party Normalization 8-15
Setting the Service Parameters for Calling Party Normalization 8-15
Configuring the Calling Party Number Type 8-17
Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows 8-18
Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number 8-25
Providing Information to End Users 8-26
Related Topics 8-27

CHAPTER 9
Cisco Extension Mobility 9-1
Configuration Checklist for Cisco Extension Mobility 9-1
Introducing Cisco Extension Mobility 9-5
Understanding Device Profiles 9-5
User Device Profile 9-6
Default Device Profile 9-6
Overview of Cisco Extension Mobility 9-6
Login and Logout Behavior 9-8
Login Call Flow 9-9
Logout Call Flow 9-10
Extension Mobility Equivalency 9-11
System Requirements for Cisco Extension Mobility 9-13
Interactions and Restrictions 9-14
Interactions 9-14
Cisco Unified Communications Manager Services That Are Running on the Same Server 9-14
Bulk Administration Tool 9-14
Cisco Unified Communications Manager Assistant 9-15
Call Display Restrictions 9-15
Intercom 9-15
Internet Protocol Version 6 (IPv6) 9-16
Restrictions 9-16
Installing Cisco Extension Mobility for the First Time 9-17
Configuring Cisco Extension Mobility 9-17
Configuration Guidelines 9-17
Configuration Example 1 9-18
Configuration Example 2 9-18
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSVP Agent-Based CAC Basic Call</td>
<td>10-30</td>
</tr>
<tr>
<td>RSVP Agent CAC Hold/Resume by Home Phone</td>
<td>10-31</td>
</tr>
<tr>
<td>RSVP Agent CAC Hold/Resume by Visiting Phone</td>
<td>10-32</td>
</tr>
<tr>
<td>EM CC Common Call-Processing Issues</td>
<td>10-32</td>
</tr>
<tr>
<td>Obtaining Help for EM CC Call-Processing Issues</td>
<td>10-33</td>
</tr>
<tr>
<td>Phone Behavior With EM CC</td>
<td>10-33</td>
</tr>
<tr>
<td>WAN Network Failure—Configuration File Unavailable</td>
<td>10-34</td>
</tr>
<tr>
<td>EM CC Failure—Registration Rejection</td>
<td>10-35</td>
</tr>
<tr>
<td>EM CC Failure—Home Cisco Unified Communications Manager Unavailable/Interoffice Failure</td>
<td>10-36</td>
</tr>
<tr>
<td>EM CC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure</td>
<td>10-37</td>
</tr>
<tr>
<td>EM CC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure (No Visiting SRST)</td>
<td>10-38</td>
</tr>
<tr>
<td>Phone Security With EM CC</td>
<td>10-38</td>
</tr>
<tr>
<td>System Requirements for EM CC</td>
<td>10-38</td>
</tr>
<tr>
<td>Interactions and Restrictions</td>
<td>10-39</td>
</tr>
<tr>
<td>EM CC Interactions</td>
<td>10-39</td>
</tr>
<tr>
<td>EM CC Restrictions</td>
<td>10-40</td>
</tr>
<tr>
<td>Installing and Activating EM CC</td>
<td>10-41</td>
</tr>
<tr>
<td>Configuring EM CC</td>
<td>10-42</td>
</tr>
<tr>
<td>Configuring EM CC Feature Configuration Settings</td>
<td>10-42</td>
</tr>
<tr>
<td>EM CC Intercluster Service Profile Configuration Settings</td>
<td>10-47</td>
</tr>
<tr>
<td>Remote Cluster Configuration Settings</td>
<td>10-48</td>
</tr>
<tr>
<td>Providing Information to End Users</td>
<td>10-50</td>
</tr>
<tr>
<td>Troubleshooting EM CC</td>
<td>10-50</td>
</tr>
<tr>
<td>Error Codes for the Cisco Extension Mobility Application (EM App)</td>
<td>10-50</td>
</tr>
<tr>
<td>Error Codes for the Cisco Extension Mobility Service (EM Service)</td>
<td>10-51</td>
</tr>
<tr>
<td>Related Topics</td>
<td>10-54</td>
</tr>
</tbody>
</table>

### Chapter 11

**Cisco Unified Communications Manager Assistant With Proxy Line Support**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Checklist for Cisco Unified Communications Manager Assistant with Proxy Line Support</td>
<td>11-1</td>
</tr>
<tr>
<td>Introducing Cisco Unified Communications Manager Assistant</td>
<td>11-2</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant Architecture Overview</td>
<td>11-5</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant Service</td>
<td>11-6</td>
</tr>
<tr>
<td>Cisco IP Manager Assistant Service</td>
<td>11-7</td>
</tr>
<tr>
<td>Assistant Console Interface</td>
<td>11-8</td>
</tr>
<tr>
<td>Cisco Unified IP Phone Interface</td>
<td>11-9</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant Database Access Architecture</td>
<td>11-10</td>
</tr>
</tbody>
</table>
Manager Interfaces 11-10
Assistant Interfaces 11-10
Softkeys 11-11
Cisco Unified Communications Manager Assistant Administration Interface 11-11
System Requirements for Cisco Unified Communications Manager Assistant with Proxy Line Support 11-12
Devices That Support Cisco Unified Communications Manager Assistant 11-12
Interactions and Restrictions 11-13
Interactions 11-13
Bulk Administration Tool 11-13
Calling Party Normalization 11-14
Extension Mobility 11-14
Internet Protocol Version 6 (IPv6) 11-14
Reporting Tools 11-14
Multilevel Precedence and Preemption (MLPP) 11-15
Time-of-Day Routing 11-16
Message Waiting Indicator 11-16
Intercom 11-16
Restrictions 11-16
Installing and Activating Cisco Unified Communications Manager Assistant 11-17
Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support 11-18
System Configuration with Proxy Line Support 11-18
Cisco Unified Communications Manager Assistant Configuration Wizard 11-19
Calling Search Space and Partitions 11-22
Cisco Unified Communications Manager Assistant CTI Route Point 11-23
Setting the Service Parameters for Cisco Unified Communications Manager Assistant 11-24
Configuring Multiple Servers for Cisco Unified Communications Manager Assistant 11-27
Scalability 11-27
Security Considerations 11-28
Starting the Cisco IP Manager Assistant Service 11-29
Cisco Unified IP Phone Service Configuration 11-29
Manager and Assistant Phone Configuration 11-29
Manager Phones 11-30
Assistant Phones 11-31
Nonmanager and Nonassistant Phones 11-33
Manager and Assistant Configuration 11-33
Configuring a Manager and Assigning an Assistant for Proxy Line Mode 11-34
Deleting Cisco Unified Communications Manager Assistant Information from the Manager 11-36
Updating the Manager Cisco Unified Communications Manager Assistant Configuration 11-37
Cisco Unified Communications Manager Assistant With Shared Line Support

Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support

Introducing Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant Architecture Overview

Cisco IP Manager Assistant Service

Assistant Console Interface

Cisco Unified IP Phone Interface

Cisco Unified Communications Manager Assistant Database Access Architecture

Manager Interfaces

Assistant Interfaces

Softkeys

Cisco Unified Communications Manager Assistant Administration Interface

System Requirements for Cisco Unified Communications Manager Assistant with Shared Line Support

Devices That Support Cisco Unified Communications Manager Assistant

Interactions and Restrictions

Interactions

Bulk Administration Tool

Calling Party Normalization

Extension Mobility

Internet Protocol Version 6 (IPv6)

Reporting Tools

Multilevel Precedence and Preemption (M LPP)

Intercom

Restrictions

Installing and Activating Cisco Unified Communications Manager Assistant
Configuring Cisco Unified Communications Manager Assistant with Shared Line Support 12-15

Setting the Service Parameters for Cisco Unified Communications Manager Assistant 12-16

Configuring Multiple Servers for Cisco Unified Communications Manager Assistant 12-18

Scalability 12-18

Security Considerations 12-19

Starting the Cisco IP Manager Assistant Service 12-19

Manager and Assistant Phone Configuration 12-19

Manager Phones 12-20

Assistant Phones 12-21

Nonmanager and Nonassistant Phones 12-21

Manager and Assistant Configuration 12-21

Configuring a Manager and Assigning an Assistant for Shared Line Mode 12-22

Deleting Cisco Unified Communications Manager Assistant Information for the Manager 12-24

Updating the Manager Cisco Unified Communications Manager Assistant Configuration 12-24

Configuring Shared and Incoming Intercom Lines for the Assistant 12-25

Deleting the Cisco Unified Communications Manager Assistant Information for the Assistant 12-27

Updating the Assistant Cisco Unified Communications Manager Assistant Configuration 12-27

Dial Rules Configuration 12-28

Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants 12-28

Installing the Assistant Console Plug-in 12-29

Assistant Console Dialog Options 12-30

Manager Configuration 12-31

Related Topics 12-31

Cisco Unified Communications Manager Auto-Attendant 13-1

Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant 13-2

Introducing Cisco Unified Communications Manager Auto-Attendant 13-3

Cisco Unified Communications Manager Auto-Attendant Overview 13-4

Components of Cisco Unified Communications Manager Auto-Attendant 13-5

System Requirements for Cisco Unified Communications Manager Auto-Attendant 13-5

Installing the Cisco Unified Communications Manager Auto-Attendant 13-6

Configuring Cisco Unified Communications Manager Auto-Attendant and the Cisco CRS Engine 13-6

Managing Cisco Unified Communications Manager Auto-Attendant 13-6

Related Topics 13-7

Cisco Unified Mobility 14-1

Configuration Checklist for Cisco Unified Mobility 14-2
Introducing Cisco Unified Mobility 14-4
   Definitions 14-5
List of Cisco Unified Mobility Features 14-6
Other Benefits of Cisco Unified Mobility Features 14-7
Mobile Connect 14-8
Desktop Call Pickup 14-10
Send Call to Mobile Phone 14-10
Mobile Voice Access 14-11
Midcall Enterprise Feature Access Support Using DTM F 14-12
Two-Stage Dialing 14-12
Time-of-Day Access 14-12
   Time-of-Day Access Configuration 14-13
   Important Notes for Time-of-Day Access 14-14
Directed Call Park via DTM F 14-15
SIP URI Dialing 14-16
Intelligent Session Control 14-17
Session Handoff 14-19
Use Case Scenarios for Cisco Unified Mobility Features 14-21
   Use Case Scenarios for Mobile Connect 14-21
   Use Case Scenarios for Mobile Voice Access 14-22
   Use Case Scenarios for Time-of-Day Access 14-22
   Use Case Scenarios for Directed Call Park via DTM F 14-23
   Use Case Scenarios for Intelligent Session Control 14-24
   Use Case Scenarios for Session Handoff 14-26
Interactions and Limitations 14-27
   Interactions 14-28
   Limitations 14-30
System Requirements 14-34
Migrating from Cisco Unified Mobility Manager 14-35
Configuring Cisco Unified Mobility 14-35
   Access List Configuration 14-36
      Access List Configuration Settings 14-36
      Access List Member Detail Configuration Settings 14-38
   Remote Destination Profile Configuration 14-39
      Remote Destination Profile Configuration Settings 14-39
      Associating a Directory Number with a Remote Destination Profile 14-43
   Remote Destination Configuration 14-43
      Remote Destination Configuration Settings 14-44
   Mobile Voice Access Directory Number Configuration 14-48
### Chapter 16: Cisco Mobile VoIP Client Features

- **Definition** 16-3
- **List of Cisco Mobile VoIP Client Features** 16-3
- **Direct Connection from Cisco Unified Communications Manager to Mobile Client Without Proxy Server** 16-4
- **DVO Optimization Settings for Toll Reduction** 16-5
- **Enable/Disable Mobile Connect From Mobile Phone** 16-6

#### Interactions and Limitations 16-6

#### System Requirements 16-6

**Configuring Cisco Mobile VoIP Clients** 16-6

**Related Topics** 16-7

### Chapter 17: Cisco Web Dialer

**Configuration Checklist for Cisco Web Dialer** 17-1

**Introducing Cisco Web Dialer** 17-2
- **Webdialer Servlet** 17-2
- **Redirector Servlet** 17-3

**Redundancy** 17-3

**System Requirements for Cisco Web Dialer** 17-4

#### Interactions and Restrictions 17-4
- **Interactions** 17-4
- **Restrictions** 17-5

#### Installing and Activating Cisco Web Dialer 17-5

**Configuring Cisco Web Dialer** 17-6
- **Configuring the Webdialer Servlet** 17-6
- **Setting Service Parameters for the Webdialer Servlet** 17-6
- **Configuring Cisco Web Dialer in the Application Server Window** 17-8
- **Configuring the Application User** 17-9
  - **Secure TLS Connection to CTI** 17-9
- **Configuring Web Dialer for the Local Language** 17-10
- **Partition Support** 17-11
- **Configuring the Redirector Servlet (Optional)** 17-11
- **Configuring Application Dial Rules (Optional)** 17-11
- **Adding Users to the Standard Cisco Unified Communications Manager End Users Group** 17-12
- **Creating a Proxy User (Optional)** 17-12
- **Trace Settings (optional)** 17-14

**Related Topics** 17-14
CHAPTER 18  Client Matter Codes and Forced Authorization Codes  18-1

Configuration Checklist for Client Matter Codes and Forced Authorization Codes  18-2
Introducing Client Matter Codes  18-2
Introducing Forced Authorization Codes  18-3
Interactions and Restrictions  18-4
  Using the Cisco Bulk Administration Tool  18-5
  Using CDR Analysis and Reporting  18-6
  Using FAC/CMC with CTI, JTAPI, and TAPI Applications  18-6
System Requirements  18-6
Installation of CMC and FAC  18-6
Configuring Client Matter Codes  18-7
  CMC Configuration Settings  18-7
  Enabling Client Matter Codes For Route Patterns  18-8
Configuring Forced Authorization Codes  18-9
  FAC Configuration Settings  18-9
  Enabling Forced Authorization Codes for Route Patterns  18-10
Providing Information to Users  18-11
Related Topics  18-11

CHAPTER 19  Custom Phone Rings  19-1

Introducing Custom Phone Rings  19-1
Customizing and Modifying Configuration Files  19-2
Ringlist.xml File Format Requirements  19-2
PCM File Requirements for Custom Ring Types  19-3
Configuring a Custom Phone Ring  19-3
Related Topics  19-3

CHAPTER 20  Device Mobility  20-1

Configuration Checklist for Device Mobility  20-2
Introducing Device Mobility  20-3
Understanding How Device Mobility Works  20-3
  Device Mobility Operations Summary  20-5
  Device Mobility Groups Operations Summary  20-6
Network Considerations  20-7
Interactions and Restrictions  20-8
System Requirements  20-9
  Devices That Support Device Mobility  20-9
Installing Device Mobility 20-10
Configuring Device Mobility 20-10
Configuration Tips for Device Mobility 20-11
Enabling Device Mobility 20-12
Finding a Physical Location 20-12
Configuring a Physical Location 20-13
Physical Location Configuration Settings 20-14
Deleting a Physical Location 20-15
Finding Device Mobility Groups 20-15
Configuring a Device Mobility Group 20-16
Device Mobility Group Configuration Settings 20-17
Deleting a Device Mobility Group 20-17
Finding Device Mobility Info 20-18
Configuring Device Mobility Information 20-19
Device Mobility Info Configuration Settings 20-19
Deleting a Device Mobility Info 20-20
Configuring Device Pools for Device Mobility 20-21
Viewing Roaming Device Pool Parameters 20-21
Related Topics 20-21

CHAPTER 21
Do Not Disturb 21-1
Configuration Checklist for Do Not Disturb 21-1
Introducing Do Not Disturb 21-2
Incoming Call Alert Settings 21-2
Overview of Do Not Disturb Architecture 21-3
DND Status Notification for SIP Devices 21-3
DND Status Notification for SCCP Devices 21-3
System Requirements for Do Not Disturb 21-3
Software Requirements 21-3
Hardware Requirements 21-4
Devices That Support Do Not Disturb 21-4
Interactions and Restrictions 21-5
Interactions 21-5
Call Forward All 21-5
Park Reversion 21-5
Pickup 21-6
Hold Reversion and Intercom 21-6
MLPP and CER 21-6
Callback 21-6
Pickup Notification 21-6
Hunt List 21-6
Extension Mobility 21-7
Restrictions 21-7
Installing and Activating Do Not Disturb 21-7
Configuring Do Not Disturb 21-7
Setting the Do Not Disturb Service Parameters 21-8
Configuring DND Softkeys 21-8
Configuring a DND Button 21-9
Configuring Device Parameters for DND 21-9
Adding DND to Common Phone Profiles 21-11
How to Use Do Not Disturb 21-11
Using the Do Not Disturb Feature 21-12
Do Not Disturb Usage Examples 21-12
DND Ringer Off Option 21-12
DND Call Reject Option 21-15
Troubleshooting Do Not Disturb 21-16
Basic DND Troubleshooting 21-16
Troubleshooting Phones That Are Running SIP 21-17
Troubleshooting Phones That Are Running SCCP 21-17
Troubleshooting DND Errors 21-17
Related Topics 21-18

CHAPTER 22
External Call Control 22-1
Configuration Checklist for External Call Control 22-2
Introducing External Call Control for Cisco Unified Communications Manager 22-5
Cisco Unified Communications Manager Connections to the Adjunct Route Server(s) 22-7
External Call Control Profiles 22-8
Chaperone Support for Routing Rules 22-9
Announcement Support for Routing Rules 22-10
System Requirements for External Call Control 22-10
Interactions and Restrictions 22-10
Installing and Activating External Call Control 22-13
Configuring External Call Control 22-13
Service Parameters for External Call Control 22-13
External Call Control Profile Configuration Settings 22-15
Finding Configuration Records for External Call Control Profiles 22-19
Configuring an External Call Control Profile 22-20
Assigning the External Call Control Profile to the Translation Pattern 22-21
Deleting Configuration Records for External Call Control Profiles 22-21
Importing the Adjunct Route Server Certificate 22-22
Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export 22-22
Providing Information to End Users 22-23
Troubleshooting External Call Control 22-23
Related Topics 22-23

CHAPTER 23 External Call Transfer Restrictions 23-1
Configuration Checklist for External Call Transfer Restrictions 23-1
Introducing External Call Transfer Restrictions 23-2
System Requirements for External Call Transfer Restrictions 23-5
Interactions and Restrictions 23-5
  Interactions 23-5
  Restrictions 23-6
Installing and Activating External Call Transfer Restrictions 23-6
Configuring External Call Transfer Restrictions 23-6
  Configuring External Call Transfer Restrictions Service Parameters 23-7
    Configuring Transfer Capabilities by Using Call Classification Service Parameter 23-7
    Setting the Block OffNet to OffNet Transfer Service Parameter 23-7
  Configuring Transfer Capabilities by Using Gateway Configuration 23-8
  Configuring Transfer Capabilities by Using Trunk Configuration 23-8
  Configuring Transfer Capabilities by Using Route Pattern Configuration 23-9
Related Topics 23-9

CHAPTER 24 Geolocations and Location Conveyance 24-1
Configuration Checklist for Geolocations 24-1
Configuration Checklist for Geolocation Filters 24-3
Configuration Checklist for Location Conveyance 24-4
Introducing Geolocations 24-5
  Overview of Geolocations 24-6
    Geolocation Characteristics 24-6
    Geolocation Usage for Shared Lines and Route Lists 24-8
    Geolocation Examples 24-8
    Geolocation Identifiers 24-8
  Geolocation Interactions 24-9
  Geolocation Configuration 24-10
  Finding a Geolocation 24-10
CHAPTER 24  24-1

Configuring a Geolocation  24-11
Deleting a Geolocation  24-12
Geolocation Configuration Settings  24-12

Introducing Geolocation Filters  24-16
Geolocation Filter Configuration  24-17
Finding a Geolocation Filter  24-17
Configuring a Geolocation Filter  24-18
Deleting a Geolocation Filter  24-19
Geolocation Filter Configuration Settings  24-20

Introducing Location Conveyance  24-21
Geolocation Conveyance Across SIP Trunks and Intercluster Trunks  24-22
SIP Trunk Error Handling for Geolocation Information  24-22
Intercluster Trunk Error Handling for Geolocation Information  24-23
Handling a Received Geolocation  24-23
Feature Interactions with Midcall Geolocation Change  24-23
Location Conveyance Configuration  24-25
Related Topics  24-25

CHAPTER 25  25-1

Hold Reversion  25-1
Configuration Checklist for Hold Reversion  25-1
Introducing Cisco Hold Reversion  25-2
Understanding How Cisco Hold Reversion Works  25-3
Hold Reversion Alerting Operations  25-4
Call Focus Operations  25-5
How to Retrieve Reverted Calls  25-5
Timer Deactivation  25-6
Examples  25-6
System Requirements  25-8
Devices That Support Hold Reversion  25-8
Interactions and Restrictions  25-9
Interactions  25-9
Music on Hold  25-9
Call Park  25-9
MLPP  25-10
CTI Applications  25-10
Restrictions  25-10
Installing and Activating Cisco Hold Reversion  25-11
Configuring Cisco Hold Reversion  25-11
Immediate Divert Scenarios With Use Legacy Immediate Divert Service Parameter Set to False 27-7

Interactions and Restrictions 27-7

Interactions 27-8
  Multilevel Precedence and Preemption (MLPP) 27-8
  Call Forward 27-8
  Call Detail Records (CDR) 27-8
  Conference 27-8
  Hunt List 27-8

Restrictions 27-9

Installing and Activating Immediate Divert 27-10

Configuring Immediate Divert 27-10
  Setting the Service Parameters for Immediate Divert 27-10

Related Topics 27-11

CHAPTER 28

Intercom 28-1

Configuration Checklist for Intercom 28-1

Introducing Intercom 28-2

System Requirements 28-4
  Intercom Support for Cisco Unified IP Phones 28-4

Call and Line States 28-4

Interactions and Restrictions 28-5

Interactions 28-5
  Bulk Administration Tool 28-6
  Barge 28-6
  Do Not Disturb (DND) 28-6
  Call Preservation 28-6
  Cisco Unified Survivable Remote Site Telephony (SRST) 28-6
  Cisco Unified Communications Manager Assistant 28-6
  CTI 28-6
  Cisco Extension Mobility 28-7
  Internet Protocol Version 6 (IPv6) 28-7

Restrictions 28-7

Installing and Activating Intercom 28-7

Configuring Intercom 28-8
  Intercom Partition Configuration 28-8
    Adding an Intercom Partition 28-9
    Finding an Intercom Partition 28-9
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an Intercom Partition</td>
</tr>
<tr>
<td>Intercom Partition Configuration Settings</td>
</tr>
<tr>
<td>Synchronizing an Intercom Partition With Affected Devices</td>
</tr>
<tr>
<td>Deleting an Intercom Partition</td>
</tr>
<tr>
<td>Intercom Calling Search Space Configuration</td>
</tr>
<tr>
<td>Finding an Intercom Calling Search Space</td>
</tr>
<tr>
<td>Configuring an Intercom Calling Search Space</td>
</tr>
<tr>
<td>Intercom Calling Search Space Configuration Settings</td>
</tr>
<tr>
<td>Deleting an Intercom Calling Search Space</td>
</tr>
<tr>
<td>Intercom Translation Pattern Configuration</td>
</tr>
<tr>
<td>Finding an Intercom Translation Pattern</td>
</tr>
<tr>
<td>Configuring an Intercom Translation Pattern</td>
</tr>
<tr>
<td>Intercom Translation Pattern Configuration Settings</td>
</tr>
<tr>
<td>Deleting an Intercom Translation Pattern</td>
</tr>
<tr>
<td>Intercom Directory Number Configuration</td>
</tr>
<tr>
<td>Intercom Directory Number Configuration Overview</td>
</tr>
<tr>
<td>Finding an Intercom Directory Number</td>
</tr>
<tr>
<td>Configuring an Intercom Directory Number</td>
</tr>
<tr>
<td>Intercom Directory Number Configuration Settings</td>
</tr>
<tr>
<td>Synchronizing an Intercom Directory Number With Affected Devices</td>
</tr>
<tr>
<td>Deleting an Intercom Directory Number</td>
</tr>
<tr>
<td>Intercom Line and Speed Dial Configuration</td>
</tr>
<tr>
<td>How to Use Intercom</td>
</tr>
<tr>
<td>Case Studies</td>
</tr>
<tr>
<td>Illustrated Explanation of Intercom</td>
</tr>
<tr>
<td>Scenario 1</td>
</tr>
<tr>
<td>Scenario 2</td>
</tr>
<tr>
<td>Scenario 3</td>
</tr>
<tr>
<td>Scenario 4</td>
</tr>
<tr>
<td>Scenario 5</td>
</tr>
<tr>
<td>Related Topics</td>
</tr>
</tbody>
</table>

Chapter 29

Internet Protocol Version 6 (IPv6) | 29-1 |
| Configuration Checklist for IPv6 | 29-2 |
| Introducing IPv6 for Cisco Unified Communications Manager | 29-5 |
| CTI Applications | 29-5 |
| Cisco Unified Communications Manager | 29-6 |
| Cisco Unified IP Phones | 29-8 |
| DHCPv6 | 29-10 |
| DNS | 29-11 |
Gateways 29-12
Media Termination Points 29-12
SIP Trunks 29-13
TFTP Server 29-15
System Requirements for IPv6 29-16
Interactions and Restrictions 29-16
Installing and Activating IPv6 29-21
Configuring IPv6 29-21
Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window 29-21
Configuring Service and Enterprise Parameters for IPv6 29-25
Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration 29-27
Providing Information to End Users 29-32
Troubleshooting IPv6 29-32
Related Topics 29-32

CHAPTER 30 Licensing 30-1
Checklist for Licensing 30-2
Licensing for Cisco Unified Communications Manager on VMware on Cisco UCS B-Series Blade Servers 30-3
Understanding Licensing 30-3
Understanding Licensing Terminology 30-3
Understanding Licensing-Related Windows 30-4
Understanding the Contents of the License File 30-6
Understanding How Licensing Works for Phones 30-8
Understanding How Adjunct Licensing Works 30-9
Understanding How Licensing Works for Applications 30-9
Interactions and Restrictions 30-11
Working with Licenses 30-12
Calculating the Number of Required License Units 30-12
Obtaining a License File 30-13
Obtaining Licenses for New Cisco Unified Communications Manager Nodes and Devices 30-14
Obtaining a Software Feature License 30-15
Verifying That the License Manager Service Is Running 30-15
Uploading a License File 30-16
Generating a License Unit Report 30-17
License Capabilities Assignment Configuration Settings 30-18
Finding a License Capabilities Assignment 30-19
Configuring the Capabilities Assignments for One User 30-20
CHAPTER 31
Local Route Groups 31-1
Configuration Checklist for Local Route Groups 31-1
Introducing Local Route Groups 31-3
Local Route Group 31-4
Binding a Provisioned Route Group to a Local Route Group During a Call 31-4
Routing with Local Route Groups 31-5
Simple Local Routing 31-6
Tail End Hop Off 31-9
Called Party Transformations 31-11
System Requirements for Local Route Groups 31-13
Interactions and Restrictions 31-13
Interactions 31-13
Supported Devices 31-13
Forwarding 31-14
Other Supplementary Services 31-14
Route Plan Report 31-14
Cisco Unified Mobility 31-15
Restrictions 31-15
Mixed Route Lists 31-15
Installing and Activating Local Route Groups 31-15
Configuring Local Route Groups 31-15
Setting the Local Route Group Service Parameters 31-16
Related Topics 31-16

CHAPTER 32
Logical Partitioning 32-1
Configuration Checklist for Logical Partitioning 32-1
Introducing Logical Partitioning 32-4
Applicability to Requirements From Indian Telecom Regulations 32-6
History 32-7
Overview of Logical Partitioning Architecture 32-8
Logical Partitioning Use of Geolocations and Geolocation Filters 32-8
Logical Partitioning Geolocation Usage for Shared Lines and Route Lists 32-10
Logical Partitioning Usage of Geolocation Identifiers 32-10
Enterprise Parameters for Logical Partitioning 32-10
Logical Partitioning Policies 32-11
LPPolicyManager and Policy Tree 32-13
Logical Partitioning Policy Search Algorithm 32-15
Policy Matching 32-17
Deny Policy Handling 32-18
LPSession Infrastructure and Policy Checking 32-18
Logical Partitioning Handling for a Basic Call 32-19
Logical Partitioning Interaction with Geolocation Conveyance Across SIP Trunks and Intercluster Trunks 32-19
   Logical Partitioning Handling of a Received Geolocation 32-20
   Logical Partitioning Feature Interactions with Midcall Geolocation Change 32-20
   Dynamic SIP Trunks 32-21
SIP Trunk or Intercluster Trunk Configuration Requirement for Logical Partitioning 32-21
System Requirements for Logical Partitioning 32-22
Interactions and Limitations 32-22
Interactions 32-22
   Call Forwarding 32-23
   Call Transfer 32-24
   Ad Hoc Conference, Join, Join Across Lines (JAL) 32-27
   Meet-Me Conference 32-28
   Call Pickup 32-29
   Call Park and Directed Call Park 32-30
   Cisco Extension Mobility 32-31
   Cisco Unified Mobility 32-32
   Shared Line 32-33
   Barge, cBarge, and Remote Resume 32-34
   Route Lists and Hunt Pilots 32-35
   CTI Handling 32-36
Limitations 32-37
Configuring Logical Partitioning 32-39
Geolocation Configuration 32-39
Geolocation Filter Configuration 32-39
Logical Partitioning Policy Configuration 32-40
   Finding a Logical Partitioning Policy 32-40
   Configuring a Logical Partitioning Policy 32-41
   Deleting a Logical Partitioning Policy Record 32-42
   Deleting a Logical Partitioning Policy Pair Configuration 32-42
   Updating a Logical Partitioning Policy Pair Configuration 32-43
   Logical Partitioning Policy Configuration Settings 32-43
Contents

One-Way Media and Firewalls 34-57
Call Preservation in Monitoring and Recording 34-58
Call Information and Call Display 34-58
CTI Event Delivery to Application 34-59

System Requirements for Monitoring and Recording 34-59
CTI Requirements 34-59
Hardware Requirements 34-60

Interactions and Limitations 34-60
Interactions 34-60
CTI and JTAPI/TSP Applications 34-60
Other Cisco Unified Communications Manager Features 34-61
Limitations 34-61

Configuring Monitoring and Recording 34-63
Turn on IP Phone BIB to Allow Monitoring or Recording 34-64
Add User for Monitoring or Recording Application 34-64
Add User to Groups That Allow Monitoring and Recording 34-65
Configure Tones for Monitoring or Recording (Optional) 34-66
Configure Monitoring Calling Search Space 34-67
Enable Recording for a Line Appearance 34-68
Create Recording Profile 34-69
Create SIP Profile for Recording (Optional) 34-70
Create a SIP Trunk That Points to the Recorder 34-71
Create a Route Pattern for the Recorder 34-72
Create Recorder Redundancy 34-73
Setting the Monitoring and Recording Service Parameters 34-74
Notification 34-74
Codec Usage 34-75
Built-In Bridge 34-75

Related Topics 34-75

CHAPTER 35

Multilevel Precedence and Preemption 35-1
Configuration Checklist for M LPP 35-1
Introducing M LPP 35-3
M LPP Terminology 35-4
Precedence 35-5
Executive Override Precedence Level 35-6
Executive Override Precedence Call Setup 35-7
Executive Override Precedence Calls Across the PRI 4ESS Interface 35-8
PRI 4ES UIUIE-Based M LPP Interface to DRSN 35-8
<table>
<thead>
<tr>
<th>Preemption</th>
<th>35-8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>35-9</td>
</tr>
<tr>
<td>Resource Priority Namespace Network Domain</td>
<td>35-9</td>
</tr>
<tr>
<td>Resource Priority Namespace Network Domain List</td>
<td>35-11</td>
</tr>
<tr>
<td>Location-Based M LPP</td>
<td>35-11</td>
</tr>
<tr>
<td>M LPP Over Intercluster Trunks</td>
<td>35-11</td>
</tr>
<tr>
<td>M LPP Precedence Patterns</td>
<td>35-11</td>
</tr>
<tr>
<td>M LPP Indication Enabled</td>
<td>35-12</td>
</tr>
<tr>
<td>Precedence Call Setup</td>
<td>35-12</td>
</tr>
<tr>
<td>Alternate Party Diversion</td>
<td>35-13</td>
</tr>
<tr>
<td>M LPP Preemption Enabled</td>
<td>35-15</td>
</tr>
<tr>
<td>Receiving Preemption</td>
<td>35-15</td>
</tr>
<tr>
<td>Preemption Enabled</td>
<td>35-15</td>
</tr>
<tr>
<td>Preemption Details</td>
<td>35-15</td>
</tr>
<tr>
<td>User Access Preemption</td>
<td>35-15</td>
</tr>
<tr>
<td>User Access Channel Nonpreemptable</td>
<td>35-17</td>
</tr>
<tr>
<td>Common Network Facility Preemption</td>
<td>35-17</td>
</tr>
<tr>
<td>Location-Based Preemption</td>
<td>35-19</td>
</tr>
<tr>
<td>M LPP Announcements</td>
<td>35-21</td>
</tr>
<tr>
<td>Unauthorized Precedence Announcement</td>
<td>35-22</td>
</tr>
<tr>
<td>Blocked Precedence Announcement</td>
<td>35-23</td>
</tr>
<tr>
<td>Busy Station Not Equipped for Preemption</td>
<td>35-24</td>
</tr>
<tr>
<td>Announcements Over Intercluster Trunks</td>
<td>35-24</td>
</tr>
<tr>
<td>M LPP Numbering Plan Access Control for Precedence Patterns</td>
<td>35-25</td>
</tr>
<tr>
<td>M LPP Trunk Selection</td>
<td>35-26</td>
</tr>
<tr>
<td>M LPP Hierarchical Configuration</td>
<td>35-29</td>
</tr>
<tr>
<td>Service Parameter Special Trace Configuration</td>
<td>35-29</td>
</tr>
<tr>
<td>CDR Recording for Precedence Calls</td>
<td>35-30</td>
</tr>
<tr>
<td>Line Feature Interaction</td>
<td>35-30</td>
</tr>
<tr>
<td>Call Forward</td>
<td>35-30</td>
</tr>
<tr>
<td>Call Transfer</td>
<td>35-31</td>
</tr>
<tr>
<td>Shared Lines</td>
<td>35-31</td>
</tr>
<tr>
<td>Call Waiting</td>
<td>35-31</td>
</tr>
<tr>
<td>Call Preservation</td>
<td>35-32</td>
</tr>
<tr>
<td>Automated Alternate Routing</td>
<td>35-32</td>
</tr>
<tr>
<td>MGCP and PRI Protocol</td>
<td>35-32</td>
</tr>
<tr>
<td>Secure Endpoints and Secure Communications</td>
<td>35-32</td>
</tr>
<tr>
<td>Mapping M LPP Precedence to DSCP Values</td>
<td>35-32</td>
</tr>
<tr>
<td>M LPP Supplementary Services</td>
<td>35-33</td>
</tr>
<tr>
<td>M LPP Support for Multiple Appearance Lines</td>
<td>35-33</td>
</tr>
</tbody>
</table>
Contents

Call Forwarding  35-34
Three-Way Calling  35-35
Call Transfer  35-35
Call Pickup  35-36
Hunt Pilots and Hunt Lists  35-36
Supplementary Services Support for SCCP Gateway Endpoints  35-37
System Requirements for Multilevel Precedence and Preemption  35-38
Devices That Support Multilevel Precedence and Preemption  35-38
Interactions and Restrictions  35-39
   Interactions  35-39
   Restrictions  35-40
Installing and Activating MLPP  35-41
Configuring MLPP  35-42
   Setting the Enterprise Parameters for MLPP  35-42
Related Topics  35-43

Music On Hold  36-1
   Configuration Checklist for Music On Hold  36-1
   Configuration Checklist for Multicast  36-3
   Configuration Checklist for Monitoring Music On Hold Performance  36-4
   Introducing Music On Hold  36-4
      Music On Hold Definitions  36-4
      Music On Hold Characteristics  36-6
      Music On Hold Functionality  36-7
         User Hold Example  36-8
         Transfer Hold Example  36-8
         Call Park Example  36-8
      Supported Music On Hold Features  36-8
Music On Hold Server  36-11
Music On Hold Audio Sources  36-12
   Creating Audio Sources  36-12
   Storing Audio Source Files  36-12
   Managing Audio Sources  36-13
Music On Hold System Requirements and Limits  36-15
Music On Hold Failover and Fallback  36-18
Configuring Music On Hold  36-18
Contents

Music On Hold Audio Source Configuration 36-18
  Finding a Music On Hold Audio Source 36-19
  Configuring a Music On Hold Audio Source 36-20
  Deleting a Music On Hold Audio Source 36-21
  Music On Hold Audio Source Configuration Settings 36-21

Fixed Music On Hold Audio Source Configuration 36-23
  Configuring the Fixed Music On Hold (M OH) Audio Source 36-24
  Deleting a Fixed Music On Hold (M OH) Audio Source 36-24
  Fixed Music On Hold (M OH) Audio Source Configuration Settings 36-25

Music On Hold Server Configuration 36-25
  Finding a Music On Hold Server 36-26
  Configuring a Music On Hold Server 36-27
  Resetting or Restarting a Music On Hold Server 36-27
  Synchronizing a Music on Hold Server 36-28
  Music On Hold Server Configuration Settings 36-28

Music On Hold Audio File Management Configuration 36-33
  Displaying Music On Hold Audio Files 36-33
  Uploading a Music On Hold Audio File 36-34
  Deleting a Music On Hold Audio File 36-35
  Viewing Music On Hold Server Performance 36-36
  Checking Service States 36-36

Related Topics 36-36

CHAPTER 37

Presence 37-1
  Configuration Checklist for Presence 37-1
  Introducing Presence 37-4
  Understanding How Presence Works with Phones and Trunks 37-5
  Understanding How Presence Works with Route Lists 37-6
  Understanding Presence Groups 37-7
  Understanding Presence Authorization 37-9
  Understanding How the SUBSCRIBE Calling Search Space Works 37-11
  Understanding How Presence Works with Extension Mobility 37-11
  System Requirements 37-12
  Presence Feature Interactions/Restrictions 37-12
  Configuring Presence 37-13
    Configuring Presence Service Parameters and Enterprise Parameters 37-13
    Configuring and Applying the SUBSCRIBE Calling Search Space 37-14
    Finding Presence Groups 37-15
Contents
Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communications Manager

Configuring Presence Groups 37-16
Presence Group Configuration Settings 37-17
Deleting a Presence Group 37-17
Applying a Presence Group 37-18
Presence Group and Presence Authorization Tips 37-19
Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons 37-20
Configuring BLF/SpeedDial Buttons 37-20
BLF/SpeedDial Configuration Settings 37-21
Related Topics 37-22

CHAPTER 38

Quality Report Tool 38-1
Configuration Checklist for QRT 38-2
Introducing Quality Report Tool 38-3
Components of QRT 38-3
Overview of QRT Architecture 38-4
Cisco CTIManager Interface (QBEHelper) 38-5
Cisco Unified Communications Manager Database Interface (DBL Library) 38-5
Screen Helper and Dictionary 38-5
Redundancy Manager 38-6
DB Change Notifier 38-6
SDI Trace and Alarm 38-6
System Requirements for QRT 38-6
Cisco Extended Functions Service Dependency 38-7
Multiple Cisco Extended Functions Applications in a Cluster 38-8
Securing a TLS Connection to CTI 38-8
How to Use QRT 38-9
User Interface 38-9
Extended Menu Choices 38-10
Problem Classification Categories and Reason Codes 38-11
Interactions and Restrictions 38-15
Installing and Activating QRT Functions 38-15
Configuring the QRT Feature 38-16
Creating a Softkey Template with the QRT Softkey 38-17
Configuring the QRT Softkey Template in Common Device Configuration 38-19
Adding the QRT Softkey Template in Phone Configuration 38-20
Configuring the Cisco Unified Serviceability Features 38-21
Activating the Cisco Extended Functions Service for QRT 38-22
Configuring Alarms and Traces for QRT 38-22
CHAPTER 38

Setting the Cisco Extended Functions Service Parameters for QRT 38-24
Using the QRT Viewer 38-25
QRT Reports 38-26
Providing Information to Users for the QRT Feature 38-30
Troubleshooting the QRT Feature 38-30
Related Topics 38-32

CHAPTER 39

Single Sign On 39-1
Configuration Checklist for Single Sign On 39-1
Introducing Single Sign On for Cisco Unified Communications Manager 39-2
System Requirements for Single Sign On 39-2
Installing and Activating Single Sign On 39-3
Configuring Single Sign On 39-3
  Configuring OpenAM 39-3
  Importing the OpenAM Certificate into Cisco Unified Communications Manager 39-4
  Configuring Windows Single Sign On with Active Directory and OpenAM 39-4
  Configuring Client Browsers for Single Sign On 39-4
    Configuring Internet Explorer for Single Sign On 39-5
    Configuring FireFox for Single Sign On 39-5
Running CLI Commands for Single Sign On 39-5
  utils sso enable 39-5
  utils sso disable 39-6
  utils sso status 39-7
Related Topics 39-7
Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

Note

This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:


The preface covers these topics:

• Purpose, page xxxvii
• Audience, page xxxvii
• Organization, page xxxviii
• Related Documentation, page xl
• Conventions, page xl
• Obtaining Documentation and Submitting a Service Request, page xlii
• Cisco Product Security Overview, page xlii

Purpose

The Cisco Unified Communications Manager Features and Services Guide provides the information that you need to understand, install, configure, manage, use, and troubleshoot Cisco Unified Communications Manager (formerly Cisco Unified CallManager) features.

Audience

The Cisco Unified Communications Manager Features and Services Guide provides information for network administrators who are responsible for managing the Cisco Unified Communications Manager system. This guide requires knowledge of telephony and IP networking technology.
## Organization

The following table provides an overview of the organization of this guide.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barge and Privacy</td>
<td>Provides a description and configuration procedures for the Cisco Unified Communications Manager features Barge and Privacy.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Provides a description and configuration procedures for Cisco Call Back.</td>
</tr>
<tr>
<td>Call Control Discovery</td>
<td>Provides a description and configuration procedures for the Call Control Discovery feature.</td>
</tr>
<tr>
<td>Call Display Restrictions</td>
<td>Provides a description and configuration procedures for the Call Display Restrictions feature.</td>
</tr>
<tr>
<td>Call Park and Directed Call Park</td>
<td>Provides a description and configuration procedures for the Cisco Unified Communications Manager Call Park and Directed Call Park features.</td>
</tr>
<tr>
<td>Call Pickup</td>
<td>Provides a description and configuration procedures for the Cisco Unified Communications Manager Call Pickup feature.</td>
</tr>
<tr>
<td>Call Throttling and the Code Yellow State</td>
<td>Provides a description of the call throttling feature and the service parameters you use to configure it.</td>
</tr>
<tr>
<td>Calling Party Normalization</td>
<td>Provides a description of calling party normalization.</td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>Provides a description and configuration procedures for Cisco Extension Mobility for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Cisco Extension Mobility Cross Cluster</td>
<td>Provides a description and configuration procedures for the Cisco Extension Mobility Cross Cluster feature for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant with Proxy Line Support</td>
<td>Provides a description and configuration procedures for Cisco Unified Communications Manager Assistant (Cisco Unified CM Assistant) with proxy line support.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant with Shared Line Support</td>
<td>Provides a description and configuration procedures for Cisco Unified Communications Manager Assistant (Cisco Unified CM Assistant) with shared line support.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Auto-Attendant</td>
<td>Provides a description and configuration procedures for Cisco Unified Communications Manager Auto-Attendant.</td>
</tr>
<tr>
<td>Cisco Unified Mobility</td>
<td>Provides a description and configuration information for Cisco Unified Mobility, including the Mobile Connect and Mobile Voice Access features.</td>
</tr>
<tr>
<td>Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration</td>
<td>Provides a description and configuration information for integration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Chapter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco Mobile VoIP Clients</td>
<td>Cisco Unified Communications Manager provides certain functionality for Cisco Mobile VoIP Clients that connect directly with Cisco Unified Communications Manager. This chapter discusses the features and the required configurations.</td>
</tr>
<tr>
<td>Cisco Web Dialer</td>
<td>Provides a description and configuration procedures for Cisco Web Dialer for Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Client Matter Codes and Forced Authorization Codes</td>
<td>Provides descriptions and configuration procedures for Client Matter Codes (CMC) and Forced Authorization Codes (FAC).</td>
</tr>
<tr>
<td>Custom Phone Rings</td>
<td>Provides a description and configuration procedures for Cisco Unified Communications Manager custom phone rings.</td>
</tr>
<tr>
<td>Device Mobility</td>
<td>Provides a description and configuration information for the Device Mobility feature.</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Provides a description and configuration information for the Do Not Disturb feature.</td>
</tr>
<tr>
<td>External Call Control</td>
<td>Provides a description and configuration information for the External Call Control feature.</td>
</tr>
<tr>
<td>External Call Transfer Restrictions</td>
<td>Provides a description and configuration procedures for the External Call Transfer Restrictions feature.</td>
</tr>
<tr>
<td>Geolocations and Location Conveyance</td>
<td>Provides a description and configuration procedures for geolocations, geolocation filters, and location conveyance.</td>
</tr>
<tr>
<td>Hold Reversion</td>
<td>Provides a description and configuration information for the Hold Reversion feature.</td>
</tr>
<tr>
<td>Hotline</td>
<td>Provides a description and configuration information for the Hotline feature.</td>
</tr>
<tr>
<td>Immediate Divert</td>
<td>Provides a description and configuration procedures for the Cisco Unified Communications Manager Immediate Divert feature.</td>
</tr>
<tr>
<td>Intercom</td>
<td>Provides a description and configuration information for the Cisco Unified Communications Manager Intercom feature.</td>
</tr>
<tr>
<td>Internet Protocol Version 6 (IPv6)</td>
<td>Provides information on IPv6 support for Cisco Unified Communications Manager and other components in the network.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Provides a description of how licensing works with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Local Route Groups</td>
<td>Provides a description and configuration procedures for the Local Route Groups feature.</td>
</tr>
<tr>
<td>Logical Partitioning</td>
<td>Provides a description and configuration procedures for the Logical Partitioning feature.</td>
</tr>
<tr>
<td>Malicious Call Identification</td>
<td>Provides a description and configuration procedures for the Cisco Unified Communications Manager Malicious Call Identification feature.</td>
</tr>
<tr>
<td>Monitoring and Recording</td>
<td>Provides a description and configuration information for the call monitoring and call recording features.</td>
</tr>
</tbody>
</table>
Preface

Related Documentation

See the following documents for further information about related Cisco IP telephony applications and products:

- Installing Cisco Unified Communications Manager Release 8.5(1)
- Upgrading Cisco Unified Communications Manager Release 8.5(1)
- Cisco Unified Communications Manager Documentation Guide
- Release Notes for Cisco Unified Communications Manager Release 8.5(1)
- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Call Detail Records Administration Guide
- Cisco Unified Real-Time Monitoring Tool Administration Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
- Cisco Unified Communications Solution Reference Network Design (SRND)

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
</tbody>
</table>
Notes use the following convention:

**Note**

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

Timesavers use the following conventions:

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

**Tip**

Means *the information contains useful tips*.

Cautions use the following convention:

**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 conventions:

**Warning**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.
Barge and Privacy

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey or feature button automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built in conference and shared conference bridges.

The single button barge/cBarge feature allows the user to simply press the shared-line button to be added to the call. The single button barge/cBarge feature supports built in conferences and shared conference bridges.

The administrator enables or disables privacy and privacy on hold features. Privacy must be enabled for a device to activate privacy on hold. Users toggle the privacy feature on or off.

You enable or disable the privacy setting. When privacy is enabled, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls. You can configure privacy for all devices or configure privacy for each device. Users toggle the privacy feature on or off.

The privacy on hold feature preserves privacy when a private call on a shared line is put on hold. When privacy on hold is enabled, the calling name and number that are blocked when privacy is enabled remain blocked when the call is put on hold, and the system blocks other shared lines from resuming the held call. When privacy on hold is disabled and a private call is put on hold, the system displays calling name and number on all phones that have shared line appearances and allows other shared lines to resume the held call.

If privacy on hold is enabled, users can activate the feature while the call is on hold by toggling privacy on; likewise, users can deactivate privacy on hold by toggling privacy off while the call is on hold. If privacy on hold is disabled, toggling privacy on or off does not affect the held call.

If a private call is put on hold, retrieved at the same phone, and privacy is then toggled off, the system displays the call information on all phones that have shared line appearances but does not allow another phone to resume or barge the held call.

Administrators can configure privacy for all devices or for each device. Administrators configure privacy on hold for the cluster.

This chapter provides the following information about barge and privacy:

- **Configuration Checklists for Barge**, page 1-2
- **Configuration Checklist for Privacy and Privacy on Hold**, page 1-4
- **Introducing Barge, Privacy, and Privacy on Hold**, page 1-5
- **Privacy on Hold**, page 1-10
Configuration Checklists for Barge

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

Barge adds a user to a call that is in progress. Pressing a softkey or feature button automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone (if configured). Barge supports built-in conferences and shared conference bridges.

The single button barge/cBarge feature allows the user to simply press the shared-line button to be added to the call. The single button barge/cBarge feature supports built-in conferences and shared conference bridges.
Table 1-1 provides a checklist to configure the barge feature with built in conference bridge. Table 1-2 provides a checklist to configure the barge feature with shared conference bridge. See Table 1-3 for the configuration checklist for the privacy and privacy on hold features. For more information on the barge feature, see the “Introducing Barge, Privacy, and Privacy on Hold” section on page 1-5 and the “Related Topics” section on page 1-17.

Table 1-1  Barge with Built-In Conference Bridge Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Assign the Standard User or Standard Feature softkey template (both contain the barge softkey) to each device that accesses barge by using the built in conference bridge.</td>
</tr>
<tr>
<td></td>
<td>Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Set the following optional Cisco CallManager service parameters:</td>
</tr>
<tr>
<td></td>
<td>- To enable barge for all users, set the Built In Bridge Enable clusterwide service parameter to On.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If this parameter is set to Off, configure barge for each phone by setting the Built in Bridge field in Phone Configuration</td>
</tr>
<tr>
<td></td>
<td>- Set the Party Entrance Tone clusterwide service parameter to True (required for tones) (or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window)</td>
</tr>
<tr>
<td></td>
<td>- To enable single button barge for all users, set the single button barge/cBarge Policy to barge.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If this parameter is set to Off, configure single button barge for each phone by setting the Single Button Barge field in Phone Configuration</td>
</tr>
<tr>
<td></td>
<td>- To allow a user to barge into a call when the phone is ringing or when the call is connected (the barger hears a ringback tone), set the Allow Barge When Ringing service parameter to True.</td>
</tr>
<tr>
<td></td>
<td>Configuring Service Parameters for a Service on a Server, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Party Entrance Tone and Barge, cBarge, or Single Button Barge, page 1-9</td>
</tr>
<tr>
<td></td>
<td>Directory Number Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the End User Configuration window for each user that is allowed to access the barge with built-in conference bridge feature, associate the device that has the barge softkey template that is assigned to it.</td>
</tr>
<tr>
<td></td>
<td>End User Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Notify users that the barge feature is available.</td>
</tr>
<tr>
<td></td>
<td>See the phone documentation for instructions on how users access barge on their Cisco Unified IP Phone.</td>
</tr>
</tbody>
</table>
Table 1-2 provides a checklist to configure barge with shared conference bridge.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>To create a softkey template that includes cBarge, make a copy of the Standard Feature softkey template. Modify this user-named copy to add the conference barge (cBarge) softkey to the Selected Softkeys in the Remote in Use call state. See the “Adding Non-Standard Softkey Templates” section in the Cisco Unified Communications Manager Administration Guide for more information on creating copies of standard softkey templates. Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Set the optional clusterwide service parameter Party Entrance Tone to True (required for tones), or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window. To enable single button cBarge for all users, set the single button barge/cBarge Policy to cBarge. Configuring Service Parameters for a Service on a Server, Cisco Unified Communications Manager Administration Guide. Party Entrance Tone and Barge, cBarge, or Single Button Barge, page 1-9. Directory Number Configuration Settings, Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If this parameter is set to Off, configure single button cBarge for each phone by setting the Single Button cBarge field in Phone Configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the End User Configuration window for each user that is allowed to access the cBarge with shared conference bridge feature, associate the device that has the cBarge softkey template that is assigned to it. Disable privacy on phones to allow cBarge. End User Configuration, Cisco Unified Communications Manager Administration Guide.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Notify users that the cBarge feature is available. See the phone documentation for instructions on how users access cBarge on their Cisco Unified IP Phone.</td>
</tr>
</tbody>
</table>

Configuration Checklist for Privacy and Privacy on Hold

The single button barge/cBarge, barge, privacy, and privacy on hold features work with each other. These features work with only shared lines.

The privacy on hold feature preserves privacy when a private call on a shared line is put on hold. When privacy on hold is enabled, the calling name and number that are blocked when privacy is enabled remain blocked when the call is put on hold, and the system blocks other shared lines from resuming the held call. When privacy on hold is disabled and a private call is put on hold, the system displays calling name and number on all phones that have shared line appearances and allows other shared lines to resume the held call.

You enable or disable the privacy setting. When privacy is enabled, the system removes the call information from all phones that share lines and blocks other shared lines from barging in on its calls. When privacy is disabled, the system displays call information on all phones that have shared line appearances and allows other shared lines to barge in on its calls. You can configure privacy for all devices or configure privacy for each device. Users toggle the privacy feature on or off.
If privacy on hold is enabled, users can activate the feature while the call is on hold by toggling privacy on; likewise, users can deactivate privacy on hold by toggling privacy off while the call is on hold. If privacy on hold is disabled, toggling privacy on or off does not affect the held call.

If a private call is put on hold, retrieved at the same phone, and privacy is then toggled off, the system displays the call information on all phones that have shared line appearances but does not allow another phone to resume or barge the held call.

You can configure privacy for all devices or for each device. Administrators configure privacy on hold for the cluster.

Table 1-3 provides a checklist to configure the privacy feature. Table 1-1 provides a checklist to configure the barge feature with built-in conference bridge. Table 1-2 provides a checklist to configure the barge feature with shared conference bridge. For more information on privacy, see the “Introducing Barge, Privacy, and Privacy on Hold” section on page 1-5 and the “Related Topics” section on page 1-17.

### Table 1-3 Privacy and Privacy on Hold Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| If all phones in the cluster need access to privacy, keep the setting of the Privacy Setting clusterwide service parameter to True (default) and keep the Privacy field in the Phone Configuration window to Default. Continue with the following steps. If only certain phones in the cluster need access to privacy, set the Privacy Setting service parameter to False and set the Privacy field in the Phone Configuration window to On. Continue with the following steps. | **Configuring Service Parameters for a Service on a Server**, Cisco Unified Communications Manager Administration Guide  
**Configuring Cisco Unified IP Phones**, Cisco Unified Communications Manager Administration Guide |
| **Step 2**          |                               |
| For each phone button template that has privacy, add Privacy to one of the feature buttons (some phone models use the Private button). | **Phone Button Template Configuration**, Cisco Unified Communications Manager Administration Guide |
| **Step 3**          |                               |
| For each phone user that wants privacy, choose the phone button template that contains the Privacy feature button. | **Configuring Cisco Unified IP Phones**, Cisco Unified Communications Manager Administration Guide |
| **Step 4**          |                               |
| In the End User Configuration window, for each user that does not want information about the shared-line appearances to display, associate the device that has the Privacy feature button that is assigned to it. | **End User Configuration**, Cisco Unified Communications Manager Administration Guide |
| **Step 5**          |                               |
| To configure the optional privacy on hold feature, set the Enforce Privacy Setting on Held Calls service parameter to True. | **Configuring Service Parameters for a Service on a Server**, Cisco Unified Communications Manager Administration Guide |
| **Step 6**          |                               |
| Notify users that the privacy feature and the privacy on hold feature (if configured) are available. | See the phone documentation for instructions on how users access privacy on their Cisco Unified IP Phone. |

### Introducing Barge, Privacy, and Privacy on Hold

The following sections describe barge and privacy.

- **Barge**, page 1-6
- **Single Button Barge/cBarge**, page 1-6
Barge

Barge allows a user to get added to a remotely active call that is on a shared line. Remotely active calls for a line comprise active (connected) calls that are made to or from another device that shares a directory number with the line. Barge supports this type of remote-in-use call.

Phones support barge in two conference modes:

- Built-in conference bridge at the target device (the phone that is being barged). This mode uses the barge softkey.
- Shared conference bridge. This mode uses the cBarge softkey.

By pressing the barge or cBarge softkey in the remote in use call state, the user gets added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays at the barge initiator device.

Single Button Barge/cBarge

The single button barge/cBarge feature allows a user to simply press the shared-line button of the remotely active call, to be added to the call with all parties. All parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

Phones support single button barge/cBarge in two conference modes:

- Built-in conference bridge at the target device (the phone that is being barged). This mode uses the single button barge feature.
- Shared conference bridge. This mode uses the single button cBarge feature.

By pressing the shared-line button of the remote in use call, the user gets added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call and status remain active.

If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays at the barge initiator device.

Table 1-4 describes the differences between barge with built-in conference bridge and shared conference.
### Table 1-4 Built-In and Shared Conference Bridge Differences

<table>
<thead>
<tr>
<th>Action</th>
<th>Using Barge Softkey or Single Button Barge (Built In Conference Bridge at Target Device)</th>
<th>Using cBarge Softkey or Single Button cBarge (Shared Conference Bridge)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The standard softkey template includes the softkey.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Note</strong> If the single button barge/cBarge feature is enabled, the softkey is not used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A media break occurs during barge setup.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User receives a barge setup tone, if configured.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>To Conference displays as the name at the barge initiator phone.</td>
<td>To barge XXX</td>
<td>To Conference</td>
</tr>
<tr>
<td>To Conference displays as the name at the target phone.</td>
<td>To/From Other</td>
<td>To Conference</td>
</tr>
<tr>
<td>To Conference displays as the name at the other phones.</td>
<td>To/From Target</td>
<td>To Conference</td>
</tr>
<tr>
<td>Bridge supports a second barge setup to an already barged call.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Initiator releases the call.</td>
<td>No media interruption occurs for the two original parties.</td>
<td>Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.</td>
</tr>
<tr>
<td>Target releases the call.</td>
<td>Media break occurs to reconnect initiator with the other party as a point-to-point call.</td>
<td>Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.</td>
</tr>
<tr>
<td>Other party releases the call.</td>
<td>All three parties get released.</td>
<td>Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.</td>
</tr>
<tr>
<td>Target puts call on hold and performs direct transfer, Join, or Call Park.</td>
<td>Initiator gets released.</td>
<td>Initiator and the other party remain connected.</td>
</tr>
</tbody>
</table>
Introducing Barge, Privacy, and Privacy on Hold

Chapter 1  Barge and Privacy

Barge Using Built In Conference—Single Button Barge or Barge Softkey

You can use single button barge or the barge softkey only in the remote-in-use call state. A Built In conference bridge proves advantageous because neither a media interruption nor display changes to the original call occur when the barge is being set up.

Note

To use the single button barge feature, ensure that single button barge is enabled on the device.

When the barge initiator releases the call, the barge call gets released between the barge initiator and target. The original call between the target device and the other party remains active. A barge disconnect tone (beep beep) plays to all remaining parties.

When the target device releases the call, the media between the barge initiator and the other party gets dropped briefly and then reconnects as a point-to-point call. The display changes at the barge initiator device to reflect the connected party.

When the other party releases the call, both the original call and the barge call get released.

When the barge initiator puts the call on hold, both the target device and the other party remain in the call.

When the target device puts the call on hold or in a conference or transfers it, the barge initiator gets released from the barge call while the original call also gets put on hold, in a conference, or transferred. The barge initiator can barge into a call again after the media gets reestablished at the target.

When the other party puts the call on hold or in a conference or transfers it, both the target device and the barge initiator remain in the call.

When network or Cisco Unified Communications Manager failure occurs, the barge call gets preserved (like all active calls).

Most Cisco Unified IP Phones include the Built In conference bridge capability, which barge uses.

Note

Cisco Unified IP Phones 7940 and 7960 cannot support two media stream encryptions or SRTP streams simultaneously. To prevent instability due to this condition, the system automatically disables the Built In bridge for Cisco Unified IP Phones 7940 and 7960 when the device security mode is set to encrypted. For more information, see the Cisco Unified Communications Manager Security Guide.

The following settings activate or deactivate the built-in conference bridge:

• Enable or disable the built-in bridge by setting the Cisco Unified Communications Manager clusterwide service parameter, Built-in Bridge Enable, to On or Off.

• Enable or disable the built-in bridge for each device by using the Built In Bridge drop-down list box in the Phone Configuration window (choose on, off, or default). On or off settings override the Built-in Bridge Enable service parameter. Choosing default uses the setting of the service parameter.

Note

To use barge with a built-in bridge, ensure the preceding items are enabled, privacy is disabled, and the barge softkey is assigned to each device or the single button barge feature is enabled. Otherwise, to use shared conference bridge, assign the cBarge softkey to each device or enable the single button cBarge feature.

For more information, see the “Configuring Barge, Privacy, and Privacy on Hold” section on page 1-17.
Introducing Barge, Privacy, and Privacy on Hold

Additional Information
See the “Related Topics” section on page 1-17.

Barge by Using Shared Conference—Single Button cBarge or cBarge Softkey

You can use single button cBarge or the cBarge softkey only in the remote-in-use call state. No standard softkey template includes the cBarge softkey. To access the cBarge softkey, the administrator adds it to a softkey template and then assigns the softkey template to a device.

Note
To use the single button cBarge feature, ensure that it is enabled on the device.

When the cBarge softkey, or a shared-line, gets pressed, a barge call gets set up by using the shared conference bridge, if available. The original call gets split and then joined at the conference bridge, which causes a brief media interruption. The call information for all parties gets changed to barge. The barged call becomes a conference call with the barge target device as the conference controller. It can add more parties to the conference or can drop any party. When any party releases from the call, which leaves only two parties in the conference, the remaining two parties experience a brief interruption and then get reconnected as a point-to-point call, which releases the shared conference resource.

For more information, see the “Configuring Barge, Privacy, and Privacy on Hold” section on page 1-17.

Additional Information
See the “Related Topics” section on page 1-17.

Barge Phone Display Messages

When a user initiates a barge to a SIP device, the barge initiator phone displays “To Barge <Display name> (Shared Line DN).” When a user initiates a barge to a SCCP device, the barge initiator phone displays “To Barge <Display name>.”

Party Entrance Tone and Barge, cBarge, or Single Button Barge

With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multiparty call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call.

If the controlling device, that is, the originator of the multiparty call has a built-in bridge, the tone gets played to all parties if you configured party tone entrance for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.

When a barge call gets created, the party entrance tone configuration of the barge target that shares the line with the barge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone.
When a cBarge call gets created, the party entrance tone configuration of the cBarge target that shares
the line with the cBarge initiator determines whether Cisco Unified Communications Manager plays the
party entrance tone. However, if the call for the target is an existing ad hoc conference that is in the same
cluster, the party entrance tone configuration for the ad hoc conference controller determines whether
Cisco Unified Communications Manager plays the tone.

To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure
that the controlling device for the multiparty call has a built-in bridge. In addition, either configure the
Party Entrance Tone service parameter, which supports the Cisco CallManager service and the entire
cluster, or configure the Party Entrance Tone setting per directory number in the Directory Number
Configuration window (Call Routing > Directory Number). For information on the service parameter,
click the question-mark button in the Service Parameter Configuration window. For information on the
Party Entrance Tone setting in the Directory Number Configuration window, see the “Directory Number
Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Privacy

With privacy, you can enable or disable the capability of users with phones that share the same line (DN)
to view call status and to barge the call. You enable or disable privacy for each phone or for all phones
in the cluster.

By default, the system enables privacy for all phones in the cluster. To enable all phones with privacy,
leave the clusterwide service parameter set to True and leave the phone privacy setting set to default.

To configure certain phones with access to privacy, you perform the following steps to enable or disable
privacy:

- Set a service parameter.
- Set the phone privacy setting to On.
- Add privacy button to phone button template.
- Add the phone button template that has privacy button to each device.

When the device that is configured for privacy registers with Cisco Unified Communications Manager,
the feature button on the phone that is configured with privacy gets labeled, and the status shows through
an icon. If the button has a lamp, it comes on.

When the phone receives an incoming call, the user makes the call private (so the call information does
not display on the shared line) by pressing the Privacy feature button. The Privacy feature button toggles
between on and off.

Additional Information
See the “Related Topics” section on page 1-17.

Privacy on Hold

With the privacy on hold feature, administrators can enable or disable the capability of users with phones
that share the same line (DN) to view call status and retrieve calls on hold.

Administrators enable or disable privacy on hold for all phones in the cluster. To enable privacy on hold,
you must also enable the privacy feature for the phone or for all phones. Privacy on hold activates
automatically on all private calls when privacy on hold is enabled.
By default, the system disables privacy on hold for all phones in the cluster. To enable all phones with privacy on hold, set the clusterwide privacy service parameter to True, set the clusterwide Enforce Privacy Setting on Held Calls service parameter to True, and leave the phone privacy setting to default.

To configure certain phones with access to privacy on hold, administrators set the Enforce Privacy Setting on Held Calls service parameter to True and set the Privacy setting for the phone to True:

1. Set the Enforce Privacy Setting on Held Calls service parameter to True.
2. Set a Privacy service parameter.
3. Set the phone privacy setting to On.
4. Add privacy button to phone button template.
5. Add the phone button template that has privacy button to each device.

To activate privacy on hold, users press the Hold softkey or Hold button while on a private call. To return to the call, users press the Resume softkey. The phone that put the call on hold displays the status indicator for a held call; shared lines display the status indicators for a private and held call.

**System Requirements for Barge, Privacy, and Privacy on Hold**

The barge and privacy features require the following software component to operate:

- Cisco Unified Communications Manager 5.0 or later

The single button barge/cBarge and privacy on hold features require the following software component to operate:

- Cisco Unified Communications Manager 6.1(1) or later

To determine which IP Phones support Barge by using the single button barge/cBarge feature or the barge or cBarge softkey, see the “Devices That Support Barge and Privacy” section on page 1-11.

To determine which IP Phones support privacy with the Privacy button on the phone button template, see the “Devices That Support Barge and Privacy” section on page 1-11.

---

**Note**

If the phone does not support a Privacy button, by default, the privacy for that phone remains Off (all devices sharing a line with that phone will display the phone information).

To determine which IP Phones support the built-in conference bridge capability, see the “Devices That Support Barge and Privacy” section on page 1-11.

**Devices That Support Barge and Privacy**

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support barge and privacy. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
     - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
- by choosing **File > Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
- by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all IP Phones that support built-in bridge, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Built In Bridge
   The List Features pane displays a list of all devices that support the built-in bridge feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

6. To generate a report of all devices that support privacy, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Privacy
   The List Features pane displays a list of all devices that support the Privacy feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

7. To generate a report of all devices that support single button barge, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Single Button Barge
   The List Features pane displays a list of all devices that support the Single Button Barge feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.


### Interactions and Restrictions

The following sections describe the interactions and restrictions for barge, privacy, and privacy on hold:

- **Interactions**, page 1-13
- **Restrictions**, page 1-14
Interactions

The following sections describe how barge and privacy interact with Cisco Unified Communications Manager applications and call processing:

- Barge and cBarge, page 1-13
- Barge and Call Park, page 1-13
- Barge and Join, page 1-13
- Barge, cBarge, and Single Button Barge Support for PLAR, page 1-13

Barge and cBarge

Cisco recommends that you assign either the barge or cBarge softkey to a softkey template. By having only one of these softkeys for each device, you can avoid confusion for users and potential performance issues.

Note

You can enable single button barge or single button cBarge for a device, but not both.

Barge and Call Park

When the target parks the call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).

Barge and Join

When the target joins the call with another call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).

Barge, cBarge, and Single Button Barge Support for PLAR

A barge, cBarge, or single button barge initiator can barge into a call via a shared line that is configured for PLAR; that is, the initiator can barge into the call if the barge target uses the preconfigured number that is associated with the PLAR line while on the call. Cisco Unified Communications Manager does not send the barge invocation to the PLAR line before connecting the barge call, so the barge occurs no matter what the state of the PLAR destination is.

To make barge, cBarge, or single button barge work with PLAR, you must configure barge, cBarge, or single button barge, as described in the “Configuration Checklists for Barge” section on page 1-2. In addition, you must configure the PLAR destination, a directory number that is used specifically for PLAR. The following example describes how to enable PLAR functionality for phones that are running SCCP and for phones that are running SIP.

A and A’ represent shared-line devices that you configured for barge, cBarge, or single button barge, and B1 represents the directory number for the PLAR destination. To enable PLAR functionality from A/A’, which are running SIP, see the following example:

Step 1 through Step 4 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Step 1 through Step 6.
Example for How to Configure PLAR

Step 1  
Create a partition, for example, P1, and a calling search space, for example CSS1, so CSS1 contains P1. (In Cisco Unified Communications Manager Administration, choose Call Routing > Class of Control > Partition or Calling Search Space.)

Step 2  
Create a translation pattern, for example, TP1, which contains calling search space CSS1 and partition P1. Create a null pattern (blank pattern), but make sure that you enter the directory number for the B1 PLAR destination in the Called Party Transformation Mask field. (In Cisco Unified Communications Manager Administration, choose Call Routing > Translation Pattern.)

Step 3  
Assign the calling search space, CS1, to either A or A’. (In Cisco Unified Communications Manager Administration, choose Device > Phone.)

Step 4  
Assign the P1 partition to the directory number for B1, which is the PLAR destination. (In Cisco Unified Communications Manager Administration, choose Call Routing > Directory Number.)

Step 5  
For phones that are running SIP, create a SIP dial rule. (In Cisco Unified Communications Manager Administration, choose Call Routing > Dial Rules > SIP Dial Rules. Choose 7940_7960_OTHER. Enter a name for the pattern; for example, PLAR1. Click Save; then, click Add Plar. Click Save.)

Step 6  
For phones that are running SIP, assign the SIP dial rule configuration that you created for PLAR to the phones, which, in this example, are A and A’. (In Cisco Unified Communications Manager Administration, choose Device > Phone. Choose the SIP dial rule configuration from the SIP Dial Rules drop-down list box.)

Restrictions

The following restrictions apply to Barge:

- The barge initiator cannot conference in additional callers.
- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use Barge.
- CTI does not support Barge through APIs that TAPI/JTAPI applications invoke. CTI generates events for barge when it is invoked manually from an IP phone by using the barge or cBarge softkey.
- Cisco recommends that you do not configure cBarge for a user who has barge configured. Choose only one barge method for each user.
- The original call requires G.711 codec. If G.711 is not available, use cBarge instead.
- You can assign a softkey template that contains the barge softkey to any IP phone that uses softkeys; however, some IP phones do not support the barge feature.
- Barge supports most Cisco Unified IP Phones that run SIP. See the “Devices That Support Barge and Privacy” section on page 1-11.
- A user cannot barge into an encrypted call if the phone that is used to barge is not configured for encryption. When barge fails in this case, a busy tone plays on the phone where the user initiated the barge.

If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.
If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call state equals encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to display on the authenticated devices in the call, even if the initiator phone does not support security.

Tip You can configure cBarge if you want barge functionality, but Cisco Unified Communications Manager automatically classifies the call as nonsecure.

- If you configure encryption for Cisco Unified IP Phones 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails. A tone plays on the phone to indicate that the barge failed.

A message displays in Cisco Unified Communications Manager Administration when you attempt the following configuration:

- In the Phone Configuration window, you choose **Encrypted** for the Device Security Mode (or System Default equals Encrypted), **On** for the Built In Bridge setting (or default setting equals On), and you click **Insert** or **Update** after you create this specific configuration.

- In the Enterprise Parameter window, you update the Device Security Mode parameter.

- In the Service Parameter window, you update the Built In Bridge Enable parameter.

- If the number of shared-line users in the conference is equal to or greater than the configuration for the Maximum Number of Calls setting for the device from which you are attempting to barge, the phone displays the message, Error Past Limit.

The following restrictions apply to privacy:

- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use barge.

- CTI does not support privacy through APIs that TAPI/JTAPI applications invoke. CTI generates events when privacy gets enabled or disabled from an IP phone by using the privacy feature button.

- Privacy supports most Cisco Unified IP Phones that run SIP. See the “Devices That Support Barge and Privacy” section on page 1-11.

The following restriction applies to built-in conference bridge:

- To enhance performance, disable built-in bridge or turn on privacy for those devices that do not have shared-line appearances or do not use barge.

- The initiator cannot park a call, redirect a call, or use any feature that is using the CTI/JTAPI/TSP interface. The system supports only hold and unhold.

- Built-in conference bridge supports most Cisco Unified IP Phones that run SIP. See the “Devices That Support Barge and Privacy” section on page 1-11.

The following restrictions apply to privacy on hold:

- CTI does not support privacy on hold through APIs that TAPI/JTAPI applications invoke. CTI generates events when a privacy-enabled call is put on hold and when privacy gets enabled or disabled on held calls from an IP phone by using the privacy feature button.
Install and Activating Barge, Privacy, and Privacy on Hold

Barge, privacy, and privacy on hold system features come standard with Cisco Unified Communications Manager software. The administrator activates the features after installation to make them available for system use. The following sections provide information about activating the features:

- Activating Barge with Built In Conference Bridge, page 1-16
- Activating cBarge with Shared Conference Bridge, page 1-16
- Activating Privacy, page 1-16
- Activating Privacy on Hold, page 1-16

Activating Barge with Built In Conference Bridge

To activate barge with a built-in conference bridge, add the barge softkey to a softkey template, assign the softkey template to a device, set the Built-in Bridge Enable service parameter to On, and set the party entrance tone to True. To activate the single button barge feature, you must also enable it in the Device Profile Configuration window. See the “Configuration Checklists for Barge” section on page 1-2 for details.

Note

To set barge with built-in conference bridge for all users, set the Built-in Bridge Enable service parameter to On. To set barge with built-in conference bridge for individual users, set the Built in Bridge field to On in the Phone Configuration window.

Activating cBarge with Shared Conference Bridge

To activate barge with shared conference bridge, add the cBarge softkey to a softkey template, assign the softkey template to a device, and set the party entrance tone to True. To activate the single button cBarge feature, you must also enable it on the Device Profile Configuration window. See the “Configuration Checklists for Barge” section on page 1-2 for details.

Activating Privacy

The system automatically activates privacy in the Cisco Unified Communications Manager cluster because the Privacy Setting service parameter is set to True and the phone has the privacy setting at Default. You must also add privacy to a phone button template and assign the phone button template to a device. See the “Configuration Checklist for Privacy and Privacy on Hold” section on page 1-4 for details.

Activating Privacy on Hold

The system automatically activates privacy on hold in the Cisco Unified Communications Manager cluster when the Enforce Privacy Setting on Held Calls service parameter is set to True and the phone has the privacy feature that is configured. See the “Configuration Checklist for Privacy and Privacy on Hold” section on page 1-4 for details.
Configuring Barge, Privacy, and Privacy on Hold

This section contains the following information:

- Configuration Checklists for Barge, page 1-2
- Configuration Checklist for Privacy and Privacy on Hold, page 1-4
- Setting the Service Parameters for Barge, Privacy, and Privacy on Hold, page 1-17

**Tip**

Before you configure barge or privacy, see the “Configuration Checklists for Barge” section on page 1-2 and the “Configuration Checklist for Privacy and Privacy on Hold” section on page 1-4.

Setting the Service Parameters for Barge, Privacy, and Privacy on Hold

Cisco Unified Communications Manager provides five clusterwide service parameters: Built In Bridge Enable for the built-in conference bridge capability, Privacy Setting for the privacy feature, Enforce Privacy Setting on Held Calls setting for the privacy on hold feature, single button barge/cBarge policy for single button barge/cBarge features, and Party Entrance Tone for the tones that are played during barge.

- **Built In Bridge Enable**—Default specifies Off. This parameter enables or disables the built-in conference bridge capability for phones that use the barge softkey. Set this parameter for each server in a cluster that has the Cisco CallManager service and barge is configured. If Built in Bridge is set to On in Phone Configuration, the service parameter setting gets overridden.

- **Privacy Setting**—Default specifies True. This parameter enables or disables the privacy feature for phone users who do not want to display information on shared-line appearances. Set this parameter for each server in a cluster that has the Cisco CallManager service and privacy is configured. If only certain phones need the privacy feature, set the service parameter to False and set the Privacy field to On in Phone Configuration.

  If the Privacy field in the Phone Configuration window is set to default, the phone uses the setting that is configured in the Privacy Setting service parameter.

- **Enforce Privacy Setting on Held Calls**—Default specifies False. This parameter enables or disables the privacy on hold feature for phone users who want to preserve privacy on held calls. Set this parameter for each server in a cluster that has the Cisco CallManager service and privacy is configured.

- **Single button barge/cBarge Policy**—Default specifies Off. This parameter enables or disables the single button barge/cBarge feature for phone users who want to use the barge or cBarge feature by simply pressing the line button. Set this parameter for each server in a cluster that has the Cisco CallManager service and barge is configured.

- **Party Entrance Tone**—Default specifies False. This parameter enables or disables the tones that play during barge. Set this parameter for each server in a cluster that has the Cisco CallManager service and barge (with tones) is configured.

Related Topics

- Cisco Unified IP Phone administration documentation for Cisco Unified Communications Manager
- Cisco Unified IP Phone user documentation and release notes
• Configuration Checklists for Barge, page 1-2
• Configuration Checklist for Privacy and Privacy on Hold, page 1-4
• Introducing Barge, Privacy, and Privacy on Hold, page 1-5
• System Requirements for Barge, Privacy, and Privacy on Hold, page 1-11
• Interactions and Restrictions, page 1-12
• Installing and Activating Barge, Privacy, and Privacy on Hold, page 1-16
• Configuring Barge, Privacy, and Privacy on Hold, page 1-17
• Phone Button Template Configuration, *Cisco Unified Communications Manager Administration Guide*
• Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
• Softkey Template Configuration, *Cisco Unified Communications Manager Administration Guide*
• End User Configuration, *Cisco Unified Communications Manager Administration Guide*
• Configuring Service Parameters for a Service on a Server, *Cisco Unified Communications Manager Administration Guide*
• Phone Button Template Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
• Cisco Unified IP Phones, *Cisco Unified Communications Manager System Guide*
• Programmable Line Keys, *Cisco Unified Communications Manager System Guide*
• Directory Number Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
• *Cisco Unified Communications Manager Security Guide*
CHAPTER 2

Call Back

This chapter provides information on the following topics:

- Configuration Checklist for Call Back, page 2-1
- Introducing Call Back, page 2-3
- Understanding How Call Back Works, page 2-3
- Suspend/Resume Functionality for Call Back, page 2-5
- System Requirements for Call Back, page 2-6
- Interactions and Restrictions, page 2-7
- Installing and Activating Call Back, page 2-9
- Creating a Softkey Template for the CallBack Softkey, page 2-9
- Providing Call Back Information to Users, page 2-13
- Troubleshooting Call Back, page 2-13
- Related Topics, page 2-13

Configuration Checklist for Call Back

The Call Back feature allows you to receive call-back notification on your Cisco Unified IP Phone when a called party line becomes available. You can activate call back for a destination phone that is within the same Cisco Unified Communications Manager cluster as your phone or on a remote PINX over QSIG trunks or QSIG-enabled intercluster trunks.

To receive call-back notification, a user presses the CallBack softkey or feature button while receiving a busy or ringback tone. A user can also activate call back during reorder tone, which is triggered when the no answer timer expires.
Table 2-1 shows the steps for configuring the Call Back feature. For more information on the Call Back feature, see the “Introducing Call Back” section on page 2-3 and the “Related Topics” section on page 2-13.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>If phone users want the softkeys and messages to display in a language other than English, or if you want the user to receive country-specific tones for calls, verify that you installed the locale installer.</td>
<td>Cisco Unified Communications Operating System Administration Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>In Cisco Unified Communications Manager Administration, create a copy of the Standard User softkey template and add the CallBack softkey to the following states:</td>
<td>Creating a Softkey Template for the CallBack Softkey, page 2-9</td>
</tr>
<tr>
<td>• On Hook call state</td>
<td>Phone Button Template Configuration</td>
</tr>
<tr>
<td>• Ring Out call state</td>
<td></td>
</tr>
<tr>
<td>• Connected Transfer call state</td>
<td></td>
</tr>
<tr>
<td>If the phone supports Call Back as a feature button, create a copy of the applicable phone button template and add the CallBack feature button.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>In Cisco Unified Communications Manager Administration, add the new softkey template to the Common Device Configuration.</td>
<td>Configuring CallBack Softkey Template in Common Device Configuration, page 2-10</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>In the Phone Configuration window, perform one of the following tasks:</td>
<td>Adding CallBack Softkey Template in Phone Configuration, page 2-11</td>
</tr>
<tr>
<td>• Choose the common device configuration that contains the new softkey or phone button template.</td>
<td>Phone Button Template Configuration</td>
</tr>
<tr>
<td>• Choose the new softkey template from the Softkey Template drop-down list box, or choose the new phone button template from the Phone Button Template drop-down list box.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>In the Phone Configuration window, verify that the correct user locale is configured for the Cisco Unified IP Phone(s).</td>
<td>Changing an End User Password, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Configuring Speed-Dial Buttons or Abbreviated Dialing, Cisco Unified Communications Manager Administration Guide</td>
<td>Cisco Unified Communications Operating System Administration Guide</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>If you do not want to use the default settings, configure the Call Back service parameters.</td>
<td>Setting Call Back Service Parameters, page 2-12</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>Verify that the Cisco CallManager service is activated in Cisco Unified Serviceability.</td>
<td>Cisco Unified Serviceability Administration Guide</td>
</tr>
</tbody>
</table>
Introducing Call Back

The Call Back feature allows you to receive call-back notification on your Cisco Unified IP Phone when a called party line becomes available. You can activate call back for a destination phone that is within the same Cisco Unified Communications Manager cluster as your phone or on a remote PINX over QSIG trunks or QSIG-enabled intercluster trunks.

To receive call-back notification, a user presses the CallBack softkey or feature button while receiving a busy or ringback tone. A user can also activate call back during reorder tone, which is triggered when the no answer timer expires.

The following sections provide information on the Call Back feature:
- Understanding How Call Back Works, page 2-3
- System Requirements for Call Back, page 2-6
- Interactions and Restrictions, page 2-7
- Installing and Activating Call Back, page 2-9

Understanding How Call Back Works

The following examples describe how Call Back works after an unavailable phone becomes available:
- Example: User A calls User B, who is not available, page 2-4
- Example: User A activates the Call Back feature for User B but is busy when User B becomes available, page 2-4
- Example: User A calls User B, who configured Call Forward No Answer (CFNA) to User C before call-back activation occurs, page 2-5
- Example: User A and User C call User B at the same time, page 2-5

Note

The calling phone only supports one active call back request. The called phone can support multiple call back requests.

Call Back only supports spaces and digits 0 through 9 for the name or number of the calling or called party. To work with Call Back, the name or number of the calling or called party cannot contain # or * (pound sign or asterisk).

Note

If the originating side (User A) gets reset after Call Back has been activated, then Call Back gets automatically cancelled. User A does not receive an audio alert, and the Callback notification screen does not display. If the terminating side (User B) gets reset, Call Back does not get cancelled. User A will receive an audio alert, and the Callback notification screen displays after User B becomes available.
Example: User A calls User B, who is not available

User A calls User B, who exists either in the same Cisco Unified Communications Manager cluster as User A or in a different cluster. Because User B is busy or does not reply, User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

CallBack is activated on <DN of User B>
Press Cancel to deactivate
Press Exit to quit this screen

User A presses the Exit softkey.

After User B becomes available (phone becomes on hook after busy or completes an off-hook and on-hook cycle from idle), User A receives an audio alert, and the following message displays on the phone of User A:

<DN of User B> has become available
Time HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen

User A presses the Exit softkey and then goes off hook and dials the DN of User B. User B answers the call. Users A and B go on hook.

When User A presses the CallBack softkey, the following message displays on the phone of User A:

<DN of User B> has become available
Time HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen

Note

Manually dialing a DN that has been activated with Call Back notification does not affect the Call Back status.

Example: User A activates the Call Back feature for User B but is busy when User B becomes available

User A calls User B. User B does not answer. User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

CallBack is activated on <DN of User B>
Press Cancel to deactivate
Press Exit to quit this screen

User A presses the Exit softkey.

User C then calls User A, and users A and C go on hook in an active call. User B becomes available (phone becomes on hook after busy or completes an off-hook and on-hook cycle from idle) while User A is still on an active call. User A receives an audio alert, and the following message displays on the phone of User A:

<DN of User B> has become available
Time HH:MM MM/DD/YYYY
Press Dial to call
Press Cancel to deactivate
Press Exit to quit this screen

User A can interrupt the active call to contact User B in either of two ways:

- Select Dial from the notification screen. The active call automatically gets put on hold while User A calls User B.
• Press the Exit softkey to exit the notification screen and then park (or otherwise handle) the active call. After the active call is handled, User A can press the CallBack softkey and select Dial to call User B.

Example: User A calls User B, who configured Call Forward No Answer (CFNA) to User C before call-back activation occurs
The following scenario applies to Call Forward No Answer.
The call from User A gets forwarded to User C because Call Forward No Answer is configured for User B. User A uses call back to contact User C if User C is not busy; if User C is busy, User A contacts User B.

When User B or User C becomes available (on hook), User A receives an audio alert, and a message displays on User A phone that states that the user is available.

Example: User A calls User B, who configures call forwarding to User C after User A activates call back
The following scenarios support Call Forward All, Call Forward Busy, and Call Forward No Answer.

- User A calls User B, who exists in the same Cisco Unified Communications Manager cluster as User A. User A activates call back because User B is not available. Before User B becomes available to User A, User B sets up call forwarding to User C. User A may call back User B or User C, depending on the call-forwarding settings for User B.

- User A calls User B, who exists in a different cluster. The call connects by using a QSIG trunk. User A activates call back because User B is not available. Before User B becomes available to User A, User B sets up call-forwarding to User C. One of the following events occurs:
  - If the Callback Recall Timer (T3) has not expired, User A always calls back User B.
  - After the Callback Recall Timer (T3) expires, User A may call back User B or User C, depending on the call-forwarding settings of User B.

Tip
The timer starts when the system notifies User A that User B is available. If User A does not complete the call back call during the allotted time, the system cancels call back. On the phone of User A, a message states that User B is available, even after the call back cancellation. User A can dial User B.

Example: User A and User C call User B at the same time
User A and User C call User B at the same time, and User A and User C activate call back because User B is unavailable. A call-back activation message displays on the phones of User A and User C.

When User B becomes available, both User A and User C receive an audio alert, and a message displays on both phones that states that User B is available. The User, that is, User A or User C, that presses the Dial softkey first connects to User B.

Suspend/Resume Functionality for Call Back

Call Back provides the ability of the system to suspend the call completion service if the user, who originated Call Back, is currently busy and receives call-back notification when the called party becomes available. When the originating user then becomes available, the call completion service resumes for that user.
After the originating user (User A) activates the Call Back feature, and then becomes busy when the called party (User B) becomes available, the originating PINX sends out a Suspend Callback APDU message that indicates to the peer to suspend monitoring of User B until User A becomes available again. When User A becomes available, the originating PINX sends the Resume APDU message for the terminating side to start monitoring User B again.

Note
Call Back supports the originating Suspend/Resume call-back notification for both intracluster and intercluster QSIG trunks or QSIG-enabled intercluster trunks. It also supports Suspend/Resume notification for QSIG-enabled H.225 trunks, and H.323 gateways.

The following example describes how the Suspend/Resume feature works:

Example: User A is busy when User B becomes available
User A calls User B, who exists either in the same Cisco Unified Communications Manager cluster as User A or in a different cluster. Because User B is busy or does not reply, User A activates the Call Back feature by using the CallBack softkey. The following call back activation message displays on the phone of User A:

CallBack is activated on <DN of User B>
Press Cancel to deactivate
Press Exit to quit this screen

User A presses the Exit softkey.
User A has a busy trigger set to 1.
User A becomes busy. User B then becomes available.
User A does not receive an audio alert and does not receive a call-back notification screen on the display.
The originating side (User A) sends a Suspend Callback APDU message to the terminating side (User B).
User A becomes available. The originating side sends a Resume Callback APDU message to the terminating side. This causes monitoring of User B to resume.
When User B becomes available, User A receives an audio alert, and a Callback notification screen displays.

System Requirements for Call Back
Call Back requires the following software components:

- Cisco Unified Communications Manager 5.0 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco Database Layer Monitor service that is running on the same server as the Cisco CallManager service
- Cisco RIS Data Collector service that is running on the same server as the Cisco CallManager service
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer 7 or Microsoft Internet Explorer 8 or Firefox 3.x or Safari 4.x
Interactions and Restrictions

Note

If users want the CallBack softkeys, feature buttons, and messages on the phone to display in any language other than English, or if you want the user to receive country-specific tones for calls, install the locale installer, as described in the *Cisco Unified Communications Operating System Administration Guide*.

You can use the Call Back feature with some Cisco-provided applications, such as Cisco Unified Communications Manager Assistant.

You can call the following devices and can have call back activated on them:

- Cisco Unified IP Phones 6900, 7900, 8900, and 9900 Series (except 6901 and 6911)
- Cisco VGC Phone (uses the Cisco VG248 Gateway)
- Cisco Analog Telephone Adapter (ATA) 186 and 188
- Cisco Unified Communications Manager Release 8.0 and earlier supported Call Back only on busy subscriber for Cisco VG224 endpoints. Cisco Unified Communications Manager Release 8.5 and later supports Call Back on no answer for Cisco VG224 endpoints.
- CTI route point forwarding calls to preceding phones

Tip

When a Cisco Extension Mobility user logs in or logs out, any active call completion that is associated with call back automatically gets canceled. If a called phone is removed from the system after call back is activated on the phone, the caller receives reorder tone after pressing the Dial softkey. The user may cancel or reactivate call back.

If you forward all calls to voice-messaging system, you cannot activate call back.

Note

Call Back is not supported over SIP trunks; however, Call Back is supported over QSIG-enabled SIP trunks.

To find more information about Cisco Unified IP Phones and the Call Back feature, see the phone user documentation at the following sites:

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>CallBack Softkey</th>
<th>Call Back Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6900 Series (except 6901 and 6911)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7900 Series</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone 8900 Series</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone 9900 Series</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco IP Communicator</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Additional Information on Call Back Notification with Phones That Are Running SIP

The way that call back notification works on the Cisco Unified IP Phones 7960 and 7940 that are running SIP differs from the phones that are running SCCP. The Cisco Unified IP Phones 7960 and 7940 that run SIP do not support call-back notification for on-hook/off-hook states. The only way that Cisco Unified Communications Manager would know when a line on a SIP 7960 or 7940 phone becomes available is by monitoring an incoming SIP INVITE message that Cisco Unified Communications Manager receives from the phone. After the phone sends SIP INVITE to Cisco Unified Communications Manager and the phone goes on hook, Cisco Unified Communications Manager can send an audio and call back notification screen to the Cisco Unified IP Phone 7960 and 7940 (SIP) user.

Feature Interactions with Call Forward, iDivert, and Voice-Messaging System Features

The following call states describe the expected behaviors, for the calling party, that occur when Cisco Unified Communications Manager Call Back interacts with the Call Forward, iDivert, and voice-messaging system features.

Note

The Cisco Unified IP Phones 6900, 8900, and 9900 use the Divert feature and softkey, which behaves the same as Immediate Divert (iDivert).

When a called party (Phone B) either forwards an incoming call by using Forward All, Forward Busy, or Forward No Answer; or diverts a call by using iDivert; to a voice-messaging system, the calling party (Phone A) can enter one of the following states with respect to the call back feature:

- VM-Connected state: The call gets connected to voice-messaging system. The CallBack softkey remains inactive on the calling party (Phone A) phone.
- Ring-Out state with the original called party: The voice-mail profile of the called party does not have a voice-mail pilot. The called party (Phone B) will see “Key Is Not Active” after pressing the iDivert softkey. The calling party (Phone A) should be able to activate call back against the original called party (Phone B).
- Ring-Out state with voice-messaging system feature and voice-mail pilot number as the new called party: The call encounters either voice-messaging system failure or network failure. The called party (Phone B) will see “Temp Failure” after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the “new” called party.
- Ring-Out state with busy voice-mail port and voice-mail pilot number as the new called party: The call encounters busy voice-mail port. The called party (Phone B) will see “Busy” after pressing iDivert softkey. The calling party (Phone A) cannot activate call back against the original called party (Phone B) because the call context has the voice mail pilot number as the “new” called party.
Installing and Activating Call Back

Call Back automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure Call Back in Cisco Unified Communications Manager Administration, so phone users can use the Call Back feature.

The Call Back feature relies on the Cisco CallManager services, so make sure that you activate the Cisco CallManager service in Cisco Unified Serviceability.

Configuring Call Back Softkey

The following sections provide detailed configuration information for Call Back:

- Creating a Softkey Template for the CallBack Softkey, page 2-9
- Configuring CallBack Softkey Template in Common Device Configuration, page 2-10
- Adding CallBack Softkey Template in Phone Configuration, page 2-11
- Setting Call Back Service Parameters, page 2-12

Tip
Before you configure the Call Back feature, review the “Configuration Checklist for Call Back” section on page 2-1.

Creating a Softkey Template for the CallBack Softkey

Perform the following procedure to create a new softkey template with the CallBack softkey.

Procedure

Step 1
From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Softkey Template.

The Softkey Template Configuration window displays.

Step 2
From the Find and List Softkey Template window, choose the Standard User softkey template.

Step 3
Click the Copy icon.

The Softkey Template Configuration window displays with new information.

Step 4
In the Softkey Template Name field, enter a new name for the template; for example, Standard User for Call Back.

Step 5
Click the Save button.

The Softkey Template Configuration redisplays with new information.
Step 6  To add the CallBack softkey to the template, choose **Configure Softkey Layout** from the Related Links drop-down list box in the upper, right corner and click **Go**.

The Softkey Layout Configuration window displays. You must add the CallBack softkey to the On Hook, Ring Out, and Connected Transfer call states.

Step 7  To add the CallBack softkey to the On Hook call state, choose **On Hook** from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 8  From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 9  To save and continue, click the **Save** button.

Step 10  To add the CallBack softkey to the Ring Out call state, choose **Ring Out** from the Select a Call State to Configure drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 11  From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 12  To save and continue, click the **Save** button.

Step 13  To add the CallBack softkey to the **Connected Transfer** call state, choose Connected Transfer from the Select a Call State to Configure drop-down list box.

Step 14  The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 15  From the Unselected Softkeys list, choose the CallBack softkey and click the right arrow to move the softkey to the Selected Softkeys list.

Step 16  Click the **Save** button.

---

**Configuring CallBack Softkey Template in Common Device Configuration**

Perform the following procedure to add the CallBack softkey template to the common device configuration. You create customized common device configurations for Call Back feature users.

**Procedure**

**Step 1**  From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.

The Find and List Common Device Configuration window displays.

**Step 2**  Choose any previously created common device configuration that is in the Common Device Configuration list.

**Step 3**  In the Softkey Template field, choose the softkey template that contains the CallBack softkey from the drop-down list box. (If you have not created this template, see the “Creating a Softkey Template for the CallBack Softkey” section on page 2-9.)
Adding CallBack Softkey Template in Phone Configuration

Perform the following procedure to add the CallBack softkey template to each user phone.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Phone**. The Find and List Phones window displays.

Step 2 Find the phone to which you want to add the softkey template. See “Cisco Unified IP Phone Configuration” in the *Cisco Unified Communications Manager Administration Guide*.

Step 3 Perform one of the following tasks:

- From the Common Device Configuration drop-down list box, choose the common device configuration that contains the new softkey template.
- In the Softkey Template drop-down list box, choose the new softkey template that contains the CallBack softkey.

Step 4 Click the **Save** button.

A dialog box displays with a message to press Reset to update the phone settings.

Configuring Call Back Feature Button

The following sections provide detailed configuration information for Call Back:

- Creating a Phone Button Template for the CallBack Feature Button, page 2-11
- Adding CallBack Phone Button Template in Phone Configuration, page 2-12

**Tip** Before you configure the Call Back feature, review the “Configuration Checklist for Call Back” section on page 2-1.

Creating a Phone Button Template for the CallBack Feature Button

Perform the following procedure to create a new phone button template with the CallBack feature button.

Procedure

**Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**.

The Phone Button Template Configuration window displays.
Chapter 2      Call Back

Configuring Call Back Feature Button

Step 2  From the Find and List Phone Button Template window, choose the phone button template for the IP phone that needs the Call Back feature button; for example, Standard 6961 SCCP.

Step 3  Click the Copy icon.

The Phone Button Template Configuration window displays with new information.

Step 4  In the Phone Button Template Name field, enter a new name for the template; for example, Standard 6961 SCCP for Call Back.

Step 5  Click the Save button.

The Phone Button Template Configuration redisplays with new information.

Step 6  To add the CallBack feature button to the template, choose any line button drop-down list box and choose CallBack.

Step 7  Click the Save button.

Adding CallBack Phone Button Template in Phone Configuration

Perform the following procedure to add the CallBack phone button template to each user phone.

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Device > Phone.

The Find and List Phones window displays.

Step 2  Find the phone to which you want to add the phone button template. See “Cisco Unified IP Phone Configuration” in the Cisco Unified Communications Manager Administration Guide.

Step 3  In the Phone Button Template drop-down list box, choose the new phone button template that contains the CallBack feature button.

Step 4  Click the Save button.

A dialog box displays with a message to press Reset to update the phone settings.

Setting Call Back Service Parameters

You configure Call Back service parameters by accessing System > Service Parameters in Cisco Unified Communications Manager Administration; choose the server where the Cisco CallManager service runs and then choose the Cisco CallManager service.

Unless instructed otherwise by the Cisco Technical Assistance Center, Cisco recommends that you use the default service parameters settings. Call Back includes service parameters such as Callback Enabled Flag, Callback Audio Notification File Name, Connection Proposal Type, Connection Response Type, Call Back Request Protection T1 Timer, Callback Recall T3 Timer, Callback Calling Search Space, No Path Preservation, and Set Private Numbering Plan for Callback. For information on these parameters, click the question mark button that displays in the upper corner of the Service Parameter Configuration window.
Providing Call Back Information to Users

The Cisco Unified IP Phone user guides that are available on the web provide procedures for how to use the Call Back feature on the Cisco Unified IP Phone. Use these guides in conjunction with the question mark button help provided on the Cisco Unified IP Phone 7900 Series.

Troubleshooting Call Back

Use the Cisco Unified Serviceability Trace Configuration and Real Time Monitoring Tool to help troubleshoot call back problems. See the Cisco Unified Serviceability Administration Guide and the Cisco Unified Real Time Monitoring Tool Administration Guide.

Additional Information

See the “Related Topics” section on page 2-13.

Related Topics

- Configuration Checklist for Call Back, page 2-1
- Introducing Call Back, page 2-3
- Understanding How Call Back Works, page 2-3
- Suspend/Resume Functionality for Call Back, page 2-5
- System Requirements for Call Back, page 2-6
- Interactions and Restrictions, page 2-7
- Installing and Activating Call Back, page 2-9
- Configuring Call Back Softkey, page 2-9
- Providing Call Back Information to Users, page 2-13
- Troubleshooting Call Back, page 2-13
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- Device Defaults Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Phone Button Template Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager System Guide
- Cisco Unified Serviceability Administration Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone user guides for Cisco Unified Communications Manager
The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

This chapter contains the following topics:

- Configuration Checklist for Call Control Discovery, page 3-2
- Introducing Call Control Discovery for Cisco Unified Communications Manager, page 3-5
  - Overview of Call Control Discovery, page 3-5
  - Components for the Call Control Discovery Feature, page 3-6
- System Requirements for Call Control Discovery, page 3-16
- Interactions and Restrictions, page 3-16
- Installing and Activating Call Control Discovery, page 3-18
- Configuring Call Control Discovery, page 3-18
  - Considerations for Call Control Discovery Configuration, page 3-19
  - Call Control Discovery Feature Parameters, page 3-23
  - SAF Security Profile Configuration Settings, page 3-25
  - SAF Forwarder Configuration Settings, page 3-26
  - Hosted DN Group Configuration Settings, page 3-31
  - Hosted DN Pattern Configuration Settings, page 3-32
  - CCD Advertising Service Configuration Settings, page 3-34
  - Partition Configuration Settings for Call Control Discovery, page 3-36
  - CCD Requesting Service Configuration Settings, page 3-37
  - Blocked Learned Pattern Configuration Settings, page 3-40
  - Finding Configuration Records for Call Control Discovery, page 3-42
  - Configuring Call Control Discovery (Procedure), page 3-44
The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. Table 3-1 provides a checklist for configuring the call control discovery feature in your network. Use Table 3-1 in conjunction with the “Related Topics” section on page 3-47.

**Table 3-1 Call Control Discovery Configuration Checklist**

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>If you have not already done so, configure the Cisco IOS router as the SAF forwarder.</td>
<td>See the documentation that supports your Cisco IOS router; for example, see the Cisco IOS Service Advertisement Framework Configuration Guide or the Cisco IOS Service Advertisement Framework Command Reference. Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <a href="http://www.cisco.com/go/cfn">http://www.cisco.com/go/cfn</a>.</td>
</tr>
</tbody>
</table>

| **Step 2**          |                                 |
| Configure the SAF security profile for the SAF forwarder (**Advanced Features > SAF > SAF Security Profile**). You can configure more than one SAF security profile in Cisco Unified Communications Manager Administration. A SAF forwarder, which is a Cisco IOS router that you configured for SAF, handles the publishing requests for the local Cisco Unified Communications Manager cluster and the service advertisements from remote call-control entities. | • SAF Forwarders, page 3-13  
• SAF Security Profile Configuration Settings, page 3-25  
• Considerations for Call Control Discovery Configuration, page 3-19 |
### Table 3-1  Call Control Discovery Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure the SAF forwarders in Cisco Unified Communications Manager Administration (Advanced Features &gt; SAF &gt; SAF Forwarder). Cisco recommends that you configure a primary and backup SAF forwarder for failover support.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure SAF-enabled SIP and/or H.323 intercluster (non-gatekeeper controlled) trunks (Device &gt; Trunk). The local Cisco Unified Communications Manager cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network. The Cisco Unified Communications Manager cluster advertises the SAF-enabled trunks that are assigned to the CCD advertising service along with the range of hosted DNs; therefore, when a user from a remote call-control entity makes an inbound call to a learned pattern on this Cisco Unified Communications Manager, this Cisco Unified Communications Manager receives the inbound call from this SAF-enabled trunk and routes the call to the correct DN.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure the Hosted DN groups. Cisco recommends that you group the hosted DN patterns by location; for example, hosted DN patterns that represent different zip codes for a city may get grouped together. (Call Routing &gt; Call Control Discovery &gt; Hosted DN Group) Hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. You assign a hosted DN group to a CCD advertising service in Cisco Unified Communications Manager Administration, and the CCD advertising service publishes all the hosted DN patterns that are a part of the hosted DN group. You can only assign one Hosted DN group to one call control discovery advertising service.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configure the Hosted DN patterns. (Call Routing &gt; Call Control Discovery &gt; Hosted DN Pattern) Hosted directory number (DN) patterns are patterns that represent directory numbers that belong to a call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration are a range of directory numbers that belong to the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns to the active SAF forwarder.</td>
</tr>
</tbody>
</table>
**Step 7**

To publish the hosted DNs for the local Cisco Unified Communications Manager cluster, configure the Call Control Discovery Advertising service. ([Call Routing > Call Control Discovery > Advertising Service](#)) You can configure as many CCD advertising services as you want.

The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise its hosted DNs and the PSTN failover configuration to the remote call-control entities that use the SAF network.

**Step 8**

Configure a partition that is used specifically for call control discovery. ([Call Routing > Call Control Discovery > Partition](#)) This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition.

You assign the partition to the CCD Requesting Service in Cisco Unified Communications Manager Administration.

**Tip**

The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

**Step 9**

To ensure that the local Cisco Unified Communications Manager cluster can listen for advertisements from the SAF network, configure one call control discovery requesting service. ([Call Routing > Call Control Discovery > Requesting Service](#)) You can only configure one CCD requesting service.

The call control discovery requesting service, which resides in the local Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network.

**Step 10**

If you have not already done so, configure your remote call-control entity to use the SAF network; for example, configure Cisco Unified Communications Manager Express or other Cisco Unified Communications Manager clusters for the SAF network.

See the documentation that supports your remote call-control entity; for example, the Cisco Unified Communications Manager Express documentation.

**Step 11**

After you configure call control discovery, you may block learned patterns that remote call-control entities send to the local Cisco Unified Communications Manager. ([Call Routing > Call Control Discovery > Blocked Learned Patterns](#))

See the documentation that supports your remote call-control entity; for example, the Cisco Unified Communications Manager Express documentation.
Introducing Call Control Discovery for Cisco Unified Communications Manager

This section contains information on the following topics:

- Overview of Call Control Discovery, page 3-5
- Components for the Call Control Discovery Feature, page 3-6

Overview of Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows the local Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. Additionally, the call control discovery feature enables the network to facilitate communication between SAF-supported entities, instead of relying on additional servers to enable intercall agent communications.

Tip

The call control discovery feature eliminates the need for redundant SIP proxies or complex gatekeeper configurations, which provide dial plan resolution and reachability status of remote call-control entities in the network.

With the call control discovery feature, each local Cisco Unified Communications Manager cluster can perform the following tasks:

- Establish an authenticated connection with the SAF network
- Advertise the cluster to the SAF network by providing the IPv4 address or hostname of the server, the signaling protocol and port numbers that the SAF network uses to contact the cluster, and the directory number patterns that are configured in Cisco Unified Communications Manager Administration for the cluster
- Register with the SAF network to listen for requests that are coming from other remote call-control entities that also use the SAF-related network
- Use the information that is learned from the advertisements to dynamically add patterns to its master routing table, which allows Cisco Unified Communications Manager to route and set up calls to these destinations by using the associated IP address and signaling protocol information.
- When connectivity to a remote call-control entity gets lost, the SAF network notifies Cisco Unified Communications Manager to mark the learned information as IP unreachable. The call then goes through the PSTN.
- Provide redundancy to advertise and listen for information, so if a server loses connectivity to its primary SAF forwarder for any reason, another backup SAF router can be selected to advertise and listen for information.
Components for the Call Control Discovery Feature

This section contains detailed information on the following topics:

- Call Control Discovery Terminology, page 3-6
- Call Control Discovery Advertising Service, page 3-8
  - The CCD Advertising Service and SAF-enabled Trunks, page 3-8
  - Hosted DN Patterns and the CCD Advertising Service, page 3-9
- Call Control Discovery Requesting Service, page 3-10
  - Learned Patterns and the CCD Requesting Service, page 3-10
  - The CCD Requesting Service and SAF-Enabled Trunks, page 3-11
  - Network Withdrawal Support, page 3-13
- SAF Forwarders, page 3-13

Tip: All components for the call control discovery feature work together, so review all sections to understand how the feature works.

Call Control Discovery Terminology

Table 3-2 provides a brief overview of terminology that is associated with the call control discovery feature. For detailed information on each concept, click the links in the Description column in the table.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call control discovery (CCD) advertising service         | • Resides in Cisco Unified Communications Manager  
• Advertises the PSTN failover configuration and hosted DN patterns along with the SAF trunk access information for the local Cisco Unified Communications Manager cluster to the remote call-control entities that use the SAF network.  
• Configured under Call Routing > Call Control Discovery > Advertising Service in Cisco Unified Communications Manager Administration  
• For More Information—Call Control Discovery Advertising Service, page 3-8 |
### Table 3-2 Call Control Discovery Terminology (continued)

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call control discovery (CCD) requesting service | • Resides in Cisco Unified Communications Manager  
• Allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network.  
• Ensures that learned patterns (hosted DN patterns from remote call-control entities) get inserted into digit analysis on the local Cisco Unified Communications Manager  
• Performs load balancing for calls to learned patterns  
• Handles withdrawals for Cisco Unified Communications Manager from the SAF network  
• Configured under Call Routing > Call Control Discovery > Requesting Service in Cisco Unified Communications Manager Administration.  
• For More Information—Call Control Discovery Requesting Service, page 3-10 |
| Hosted DN patterns                         | • Directory number patterns that belong to the local call-control entity  
**Tip** For example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Hosted DN Pattern are directory numbers pattern ranges for the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities.  
• For the local Cisco Unified Communications Manager, published by the CCD advertising service to the SAF forwarder.  
• For More Information—Hosted DN Patterns and the CCD Advertising Service, page 3-9 |
| Learned patterns                           | • Patterns that are inserted into digit analysis by the CCD requesting service  
• Can be manually purged or blocked on the local Cisco Unified Communications Manager  
• Viewed in RTMT  
• For More Information—Learned Patterns and the CCD Requesting Service, page 3-10 |
| SAF forwarder                              | • Cisco IOS router  
• Notifies the local Cisco Unified Communications Manager when remote call-control entities advertise their hosted DNs patterns.  
• Receives publish requests from the local Cisco Unified Communications Manager cluster so that Cisco Unified Communications Manager can advertise the hosted DN patterns for the cluster.  
• For More Information—SAF Forwarders, page 3-13 |
Introducing Call Control Discovery for Cisco Unified Communications Manager

Chapter 3 Call Control Discovery

Table 3-2 Call Control Discovery Terminology (continued)

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF-enabled trunks</td>
<td>• SAF-enabled trunks that are assigned to the CCD advertising service handle inbound calls from remote call-control entities that use the SAF network</td>
</tr>
<tr>
<td></td>
<td>• SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns</td>
</tr>
<tr>
<td></td>
<td>• For More Information—The CCD Advertising Service and SAF-enabled Trunks, page 3-8 and Learned Patterns and the CCD Requesting Service, page 3-10</td>
</tr>
</tbody>
</table>

Call Control Discovery Advertising Service

The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise the PSTN failover configuration, the hosted DN patterns, and the SAF-enabled trunk access information for its cluster to the remote call-control entities that use the SAF network. In Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Advertising Service, you can configure as many CCD advertising services as you want.

This section contains information on the following topics:

• The CCD Advertising Service and SAF-enabled Trunks, page 3-8
• Hosted DN Patterns and the CCD Advertising Service, page 3-9

The CCD Advertising Service and SAF-enabled Trunks

Consider the following information, which relates to how SAF-enabled trunks work with the CCD advertising service.

• After you configure SAF-enabled trunks in Cisco Unified Communications Manager Administration, you can choose one SIP trunk and one H.323 (non-gatekeeper controlled) trunk to associate with the CCD advertising service in the CCD Advertising Service window. The CCD advertising service advertises the hosted DN patterns, the PSTN failover configuration for the hosted DN patterns, the IP address for the node, the dynamic port number for the H.323 trunk, the QSIG configuration for the H.323 trunk, standard port 5060 for the SIP trunk, and the SIP route header information. It advertises the information for each trunk that is assigned to the CCD advertising service.

• SAF-enabled trunks do not have preconfigured destinations. For inbound calls from remote call-control entities, the local Cisco Unified Communications Manager uses the advertised dynamic trunk port number and/or SIP route header to find the proper dynamic trunk to process the call.

• The CCD advertising service, which runs on the same nodes as its assigned/selected trunks, advertises the same set of hosted DN pattern ranges for each type of trunk.

• For inbound calls from remote call-control entities to the local Cisco Unified Communications Manager, the call gets routed to the appropriate SAF-enabled trunk that is advertised by the CCD advertising service. For H.323 trunks, the incoming called party prefixes get applied to the called party number before the call gets routed.
H.323 trunks support different features than SIP trunks; for example, H.323 supports QSIG, and SIP supports presence. If your feature support requires that you assign both a H.323 and SIP trunk to the CCD advertising service, assign both trunk types. If your feature support allows you to assign one trunk type, Cisco recommends that you assign one trunk to the CCD advertising service that best serves the cluster.

If you assigned both a SAF-enabled SIP trunk and SAF-enabled H.323 (non-gatekeeper controlled) intercluster trunk to the CCD advertising service, load sharing of inbound calls occurs for the two trunks.

The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

**Hosted DN Patterns and the CCD Advertising Service**

Hosted directory numbers (DNs) patterns are a range of directory number patterns that belong to the call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Hosted DNs Pattern are directory numbers patterns for the local Cisco Unified Communications Manager that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns for the local cluster to the active SAF forwarder.

The CCD advertising service on the local Cisco Unified Communications Manager sends an advertising publish request on behalf of the hosted DN service in Cisco Unified Communications Manager to the primary SAF forwarder.

Each hosted DN pattern belongs to a hosted DN group, which you assign to the CCD advertising service. Placing hosted DN patterns into a hosted DN group ensures that a CCD advertising service can advertise multiple patterns.

When you update configured hosted DN patterns in the Hosted DN Patterns window in Cisco Unified Communications Manager Administration, the CCD advertising service resends a publishing request with the updated patterns to the active SAF forwarder. A publishing request gets sent for each trunk that is assigned to the CCD advertising service.

If a Hosted DN pattern gets added or deleted in Cisco Unified Communications Manager Administration, the CCD advertising service sends a new publish request with a higher service version number to the SAF network.

If you change the hosted DN group that is assigned to the CCD advertising service, the CCD advertising service publishes the patterns from the newly-updated hosted DN group along with a higher version number for each assigned SAF-enabled trunk.

The CCD advertising service attempts to send many hosted DN patterns in a single publishing request. If there are more hosted DN patterns than can be sent in a single request, the local Cisco Unified Communications Manager sends multiple requests, each with a unique service identifier.

For some clusters, the same hosted DN pattern may be published multiple times based on the SAF-trunk selection in the CCD advertising service configuration window. For example, hosted DN pattern 8902XXXX gets published twice for each node and each SAF-enabled trunk if the CCD advertising service configuration contains both a SAF-enabled SIP and H.323 (non-gatekeeper controlled) trunk. If the Cisco Unified Communications Manager group for the trunk contains two nodes, four publishing requests for 8902XXX get sent. This approach ensures that the receiving entity performs load sharing.

When you choose a different hosted DN group in the CCD Advertising Service window in Cisco Unified Communications Manager Administration, the service sends a request to the SAF forwarder to unpublish the hosted DN group and then publishes the updated configuration.
If a hosted DN group association changes, a SAF trunk association changes, a SAF trunk is reset in Cisco Unified Communications Manager Administration, or the CCD advertising service is reset, the CCD advertising service will unpublish the previous request and publish it again with a new service ID; in addition, other clusters receive a withdrawal service notification from the SAF network, followed by a new notification from the SAF network.

For More Information
Related Topics, page 3-47

Call Control Discovery Requesting Service

The call control discovery requesting service which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. The CCD requesting service is also responsible for inserting learned patterns from the remote call-control entities into digit analysis and the local cache. In Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Requesting Service, you can configure only one CCD requesting service.

After the SAF forwarder notifies the local Cisco Unified Communications Manager that remote call-control entities are advertising information, the CCD requesting service inserts the learned patterns along with a configured partition into digit analysis on the local Cisco Unified Communications Manager, and locally caches the learned patterns and the associated PSTN failover configuration from the remote call-control entity.

This section contains information on the following topics:
- Learned Patterns and the CCD Requesting Service, page 3-10
- The CCD Requesting Service and SAF-Enabled Trunks, page 3-11
- Network Withdrawal Support, page 3-13

Learned Patterns and the CCD Requesting Service

Remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express, request that their hosted DN patterns get advertised to other remote call-control entities. For Cisco Unified Communications Manager, after the CCD requesting service inserts the advertised DN patterns into digit analysis on the local Cisco Unified Communications Manager, Cisco Unified Communications Manager considers the pattern to be a learned pattern.

Consider the following information about learned patterns and the CCD requesting service:
- The CCD requesting service on the local Cisco Unified Communications Manager subscribes its primary SAF forwarder to the hosted DN service in order to learn about the hosted DN patterns that are advertised by the remote call-control entities. For the CCD requesting service to subscribe to the hosted DN service, you must assign a SAF-enabled trunk to the service and you must activate the service in the CCD Requesting Service Configuration window.
- If the local Cisco Unified Communications Manager receives overlapping DN patterns from remote call-control entities in single or multiple advertisements, Cisco Unified Communications Manager performs a best match for routing the call. For example, Cisco Unified Communications Manager receives patterns 813XXXX and 8135XXX. If a user dials 8135233, Cisco Unified Communications Manager routes the call to the trunk that is associated with pattern 8135XXX.
When a learned pattern from a remote call-control entity such as Cisco Unified Communications Manager Express is the same as a locally configured static pattern, the local Cisco Unified Communications Manager uses the calling search space configuration for the calling device to determine whether to route the call to the local or learned pattern.

The CCD requesting service can identify duplicate learned patterns from remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express. How the CCD requesting service handles the patterns depends on your feature parameter configuration for call control discovery in Cisco Unified Communications Manager Administration. If the Issue Alarm for Duplicate Learned Pattern feature parameter is set to True, the CCD requesting service issues an alarm and stores the duplicate learned patterns; calls that use those patterns get load balanced among different call-control entities.

If a call to a learned pattern cannot go over IP, the CCD requesting service routes the call via the PSTN. Be aware that the CCD requesting service redirects a call to the DID number based on the PSTN failover configuration for the learned pattern. If configured, the AAR calling search space for the calling device gets used to redirect the call during PSTN failover.

If the CCD requesting service receives a learned pattern that is advertised by its own cluster, Cisco Unified Communications Manager ignores the patterns; for example, if a node in the same cluster as the requesting service advertises the learned patterns, Cisco Unified Communications Manager discards the patterns.

The CCD requesting service performs regular expression checking for all learned patterns and converts lowercase wildcards to uppercase wildcards.

If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that the local Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from a remote call-control entity with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from the remote call-control entity with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by the local Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity or remote IP address, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that advertise the pattern.

You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

The CCD Requesting Service and SAF-Enabled Trunks

When you configure the CCD requesting service, you assign a SAF-enabled trunk to the service. Consider the following information on how the CCD requesting service works with SAF-enabled trunks:

- Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns from the remote call-control entities.
Introducing Call Control Discovery for Cisco Unified Communications Manager

- If the SAF-enabled trunk uses a Cisco Unified Communications Manager group with two Cisco Unified Communications Manager nodes, the CCD requesting service runs on each node after the SAF-enabled trunk registers with the Cisco Unified Communications Manager.

- When the device pool for a SAF-enabled trunk on a remote Cisco Unified Communications Manager contains three Cisco Unified Communications Manager nodes, the trunk runs on all three nodes and advertises the hosted DN service with the same DN patterns. The local Cisco Unified Communications Manager that subscribes to the Hosted DN service receives three advertisements with identical DN patterns but with different IP addresses for the 3 nodes. The CCD requesting service adds the DN patterns into its local cache and associates the patterns with the IP addresses of the three nodes. For an outbound call to a remote Cisco Unified Communications Manager, the CCD requesting service provides the dialed pattern and list of Cisco Unified Communications Managers that are associated with the DN to a SAF-enabled trunk that is assigned to the CCD requesting service. Load balancing occurs, as indicated in Table 3-3 on page 3-12. The trunk establishes the call in the order that is available to the trunk, and it goes to the next node in the list when a node is not available.

- The CCD requesting service provides the IP address and port number for the remote call-control entity to the SAF-enabled trunk.

- SAF-enabled trunks do not have preconfigured destinations. For outgoing calls to learned patterns, call control discovery provides the destination IP addresses to a dynamic trunk on a per call basis.

- The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.

- The CCD requesting service performs round-robin load balancing for calls to learned patterns by considering learned pattern protocols, its local trunks, and IP addresses of the remote call-control entity that advertised the patterns. Table 3-3 on page 3-12 shows how the CCD requesting service load balances calls to learned patterns by using SAF-enabled SIP and H.323 intercluster trunks.

### Table 3-3  Round-Robin Load Balancing for Calls to Learned Patterns

<table>
<thead>
<tr>
<th>Call</th>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the first call to 8408XXXX</td>
<td>The CCD requesting service selects the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.1/5060, 10.1.1.2/5060.</td>
</tr>
<tr>
<td>For the second call to 8408XXXX</td>
<td>The CCD requesting service selects the H323 intercluster trunk with learned H323 trunk IP addresses of 10.1.1.1/3456, 10.1.1.2/7890.</td>
</tr>
<tr>
<td>For the third call to 8408XXXX</td>
<td>The CCD requesting service selects the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.2/5060, 10.1.1.1/5060.</td>
</tr>
<tr>
<td>For the fourth call to 8408XXXX</td>
<td>The CCD requesting service selects the H.323 intercluster trunk with the learned H.323 trunk IP addresses of 10.1.1.2/7890, 10.1.1.1/3456.</td>
</tr>
</tbody>
</table>
Network Withdrawal Support

The CCD requesting service handles withdrawals from the SAF network, as described in the following bullets:

- When the remote call-control entity unpublishes specific learned patterns, the CCD requesting service purges those learned patterns from the local cache and digit analysis when it receives a source withdrawal request from the SAF network; in this case, no calls can occur to those learned patterns.

- When the SAF forwarder loses network connection with its call-control entity, the SAF forwarder withdraws those learned patterns that were published by the call control entity. In this case, CCD requesting service marks those learned patterns as unreachable via IP, and the calls gets routed through the PSTN gateway.

When a broken connection cannot be restored and if no new notification requests come in before the PSTN failover timer times out, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. In this case, no calls to these learned patterns occur.

- When the local Cisco Unified Communications Manager loses the TCP connection to both the primary and secondary SAF forwarder, the CCD requesting service marks all learned patterns as IP unreachable after the timer for the CCD Learned Pattern IP Reachable Duration feature parameter expires; in this case, all calls to learned patterns get routed through the PSTN gateway. If a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.

- When the local Cisco Unified Communications Manager loses the TCP connection to the SAF forwarder, that SAF forwarder contacts all other SAF forwarders. In this case, the other SAF forwarders notify their call control entities, and the call control entities mark their patterns as unreachable via IP after their unreachable pattern duration timer expires (for Cisco Unified Communications Manager, this is the CCD Learned Pattern IP Reachable Duration feature parameter). For Cisco Unified Communications Manager, if a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.

For More Information

Related Topics, page 3-47

SAF Forwarders

A SAF forwarder, which is a Cisco IOS router configured for SAF, notifies the local Cisco Unified Communications Manager cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local Cisco Unified Communications Manager cluster for each configured and registered trunk that is configured in the CCD Advertising Service window; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.
Table 3-4 describes the SAF deployment models that Cisco Unified Communications Manager supports.

**Table 3-4  SAF Deployment Models**

<table>
<thead>
<tr>
<th>Deployment Models</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clusterwide</td>
<td>All nodes in the cluster can connect to all SAF forwarders.</td>
<td>The clusterwide deployment model can support primary and backup SAF forwarders.</td>
</tr>
<tr>
<td>Node-specific</td>
<td>Particular nodes in the cluster are assigned to the SAF forwarders, and those nodes prioritize these SAF forwarders over other configured SAF forwarders in the network; this means that the particular nodes always contact the assigned SAF forwarders first over other configured SAF forwarders.</td>
<td>The node-specific deployment model can support primary and backup SAF forwarders. This deployment model is recommended for cluster over WAN deployments where each node in the cluster is separated geographically and you route local traffic through local nodes; for COW deployments, you can configure multiple sets of primary and backup SAF forwarders to support different geophysical locations. You can assign up to two SAF forwarders to a particular node.</td>
</tr>
</tbody>
</table>

You can configure a single SAF forwarder, which provides no failover support, or you configure a primary and backup SAF forwarder to provide failover support. With primary and backup SAF forwarders, the Cisco Unified Communications Manager advertises to and subscribes to the backup SAF forwarder when the primary SAF forwarder is unavailable.

The SAF forwarder contains the IPv4 address and port that Cisco Unified Communications Manager uses to communicate with the SAF network. At start-up time, the SAF client control, which is a nonconfigurable, inherent component of Cisco Unified Communications Manager, marks the first SAF forwarder that registers with Cisco Unified Communications Manager as the primary SAF forwarder. Be aware that the primary SAF forwarder subscribes to the hosted DN services; the backup does not perform this task. The backup SAF forwarder immediately gets promoted to the primary SAF forwarder if/when the primary SAF forwarder becomes unavailable for any reason.

The SAF client control component in Cisco Unified Communications Manager maintains the connection to the SAF forwarder by sending keepalive messages to the SAF forwarder at regular intervals. The SAF client control component experiences keepalive response timeouts with network errors, TCP connection failures, or SAF forwarder failures. When the primary SAF forwarder becomes unreachable, the backup SAF forwarder automatically becomes the primary SAF forwarder, and the SAF client component in Cisco Unified Communications Manager tries to establish a connection with the failed SAF forwarder. When the connection is successfully established, the SAF forwarder gets designated again as the backup SAF forwarder. Under these circumstances, the SAF client control component uses the newly (currently) promoted primary SAF forwarder and notifies the CCD advertising and requesting services that the current primary SAF forwarder is being used. The CCD services send all publishing and subscription requests to the current primary SAF forwarder, and the current primary SAF forwarder sends notifications for all the Hosted DN's service advertisements that it receives to the SAF client control component, which forwards the advertisements to the CCD requesting service. The CCD requesting service compares the notifications that it received from the backup SAF forwarder with its cached information and updates, deletes or adds new information, as appropriate. The SAF client control
component attempts to reconnect to the failed SAF forwarder at regular intervals. When the connection attempt is successful, the SAF client control component registers again with the previously failed SAF forwarder and redesignates the other SAF forwarder as the backup.

Cisco Unified Communications Manager always advertises to and subscribes to the primary SAF forwarder, even when you have more than 2 SAF forwarders configured in the database. If the primary SAF forwarder gets deleted from the database, then the backup SAF forwarder automatically becomes the primary SAF forwarder, and Cisco Unified Communications Manager promotes another configured SAF forwarder to the backup SAF forwarder.

For clusterwide deployments, you cannot designate the primary and backup SAF forwarders. The Cisco Unified Communications Manager database sends an ordered list of SAF forwarders to the Cisco Unified Communications Manager.

If one or both of the SAF forwarders do not work, Cisco Unified Communications Manager does not attempt to connect to a third SAF forwarder, even if a third SAF forwarder is configured. If the connection is lost for the primary and backup SAF forwarder, the Cisco Unified Communications Manager does not connect to the third SAF forwarder, even if a third SAF forwarder is configured.

If the CCD advertising or requesting service loses connection with SAF network, the SAF forwarder informs all other call control discovery services about the service interruption. The client continually attempts to register to the SAF forwarder. After the CCD service reconnects with the SAF network, the SAF forwarder immediately informs all CCD services about the service restoration.

When the SAF forwarder detects a TCP connection failure with other SAF forwarders or one of its external clients, such as Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, Cisco Unified Communications Manager marks learned patterns as unreachable after it receives a network withdrawal notification from the SAF forwarder. All subsequent calls to these learned patterns get routed over the PSTN by using the PSTN failover configuration for the unreachable learned patterns. The timer for the CCD PSTN Failover Duration feature parameter starts as soon as the network withdrawal notification is received. If Cisco Unified Communications Manager receives another network withdrawal notification when the timer is going, Cisco Unified Communications Manager restarts the timer.

Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder. You configure a SAF Forwarder security profile, which includes the username and password in requests that Cisco Unified Communications Manager sends to the SAF forwarder; the requests must include the MESSAGE INTEGRITY attribute to include the username and password.

When a connection loss occurs between the SAF forwarder and the Cisco Unified Communications Manager, for example, a cable for the server or router gets unplugged, the registration status may look correct, even when it is not. In this case, patterns may appear to be reachable until the SAF keepalive timer (on the SAF forwarder) or the TCP timer expires. After the timer for the TCP timer expires, the patterns are marked as unreachable.

For More Information
- Related Topics, page 3-47
- Cisco IOS Service Advertisement Framework Configuration Guide
- Cisco IOS Service Advertisement Framework Command Reference
System Requirements for Call Control Discovery

The following system requirements exist for Cisco Unified Communications Manager:

- Local Cisco Unified Communications Manager 8.0(2) (or higher) cluster
- SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks
- Remote call-control entities that support and use the SAF network; for example, other Cisco Unified Communications Manager 8.0(2) (or higher) clusters or Cisco Unified Communications Manager Express servers
- Cisco IOS router(s) that are configured as SAF forwarders

Tip
Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.

Interactions and Restrictions

Autonomous System
All Cisco Unified Communications Manager clusters are limited to advertised or learned routes within the same autonomous system (AS).

BLF Subscriptions
If a user wants to subscribe BLF status of a SAF learned pattern, Cisco Unified Communications Manager sends a SIP subscribe message over a SIP trunk to the remote cluster.

This functionality is supported with SAF-enabled SIP trunks only (not with SAF-enabled H.323 trunks).

Bulk Administration Tool
In the Bulk Administration Tool, you can import and export the configuration for SAF security profiles, SAF forwarder, CCD advertising service, CCD requesting service, hosted DN groups, and hosted DN patterns, and so on. For information on how to import and export the configuration, see the Cisco Unified Communications Manager Bulk Administration Guide.

Call Detail Records
Cisco Unified Communications Manager supports redirecting onBehalfOf as SAFCCDRequestingService with a redirection reason as SS_RFR_SAF_CCD_PSTNFAILOVER, which indicates that the call is redirected to a PSTN failover number.

For more information on call detail records, see the Cisco Unified Communications Manager Call Detail Records Administration Guide.

Incoming Called Party Settings
The H.323 protocol does not support the international escape character +. To ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a
inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway. See the following example for more information.

- For example, a caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

**Cisco Unified Serviceability**

Cisco Unified Serviceability provides alarms to support the call control discovery feature. For information on how to configure alarms, see the *Cisco Unified Serviceability Administration Guide*. For alarm definitions that are associated with the call control discovery feature, see the “Troubleshooting Call Control Discovery” section on page 3-47.

**Dialed Number Analyzer**

Dialed Number Analyzer allows you to add learned patterns so that you can analyze them for your dialing plan. For more information on how to perform this task, see the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

**Security (Digest Authentication)**

Cisco Unified Communications Manager uses digest authentication (without TLS) to authenticate to the SAF forwarder. When Cisco Unified Communications Manager sends a message to the SAF forwarder, Cisco Unified Communications Manager computes the SHA1 checksum and includes it in the MESSAGE-INTEGRITY field in the message.

You must configure a SAF security profile. For more information, see the “SAF Security Profile Configuration Settings” section on page 3-25.

**QSIG**

The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.

**Real Time Monitoring Tool**

The Real Time Monitoring Tool displays perfmon counters that support the call control discovery features. For information on these perfmon counters, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

The Real Time Monitoring Tool allows you to view reports for learned patterns and SAF forwarders.
Learned Pattern reports include such information as learned pattern name, time stamp, reachability status for the pattern, remote call-control entity that hosts the pattern, the PSTN failover configuration, and the destination IP address and port. RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

SAF Forwarder reports display information such as authentication status, registration status of SAF forwarders, and so on.

For more information on these reports, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

**SAF Network Issues**

When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.

In addition, Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.

## Installing and Activating Call Control Discovery

After you install Cisco Unified Communications Manager, your network can support the call control discovery feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for Call Control Discovery” section on page 3-2.

## Configuring Call Control Discovery

Before you configure the call control discovery feature, review the “Configuration Checklist for Call Control Discovery” section on page 3-2.

This section contains information on the following topics:

- Considerations for Call Control Discovery Configuration, page 3-19
- Call Control Discovery Feature Parameters, page 3-23
- SAF Security Profile Configuration Settings, page 3-25
- SAF Forwarder Configuration Settings, page 3-26
- Hosted DN Group Configuration Settings, page 3-31
- Hosted DN Pattern Configuration Settings, page 3-32
- CCD Advertising Service Configuration Settings, page 3-34
- Partition Configuration Settings for Call Control Discovery, page 3-36
- CCD Requesting Service Configuration Settings, page 3-37
Considerations for Call Control Discovery Configuration

Review the following considerations before you configure the call control discovery feature:

- SAF Forwarders, page 3-19
- Hosted DN Patterns and Hosted DN Groups, page 3-19
- CCD Advertising and Requesting Services, page 3-20
- SAF-Enabled Trunks, page 3-21

This section does not describe all configuration considerations. This section provides high-level considerations that you should review before you configure the CCD configuration settings. Use this section in conjunction with the sections that are highlighted under the “Configuring Call Control Discovery” section on page 3-18.

SAF Forwarders

- Cisco recommends that you configure a primary and backup SAF forwarder for redundancy.
- When you configure a SAF forwarder or SAF security profile, some configuration in Cisco Unified Communications Manager Administration must match the configuration that you entered on the Cisco IOS router.
- Cisco Unified Communications Manager supports the following deployment models for SAF forwarders: clusterwide or node-specific. Before you configure SAF forwarders, review Table 3-4 on page 3-14, which describes these deployment models.
- You can only configure IPv4 for SAF forwarders.
- Each SAF forwarder must have a unique IP address.
- Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.
- For information on SAF forwarder field descriptions, see the “SAF Security Profile Configuration Settings” section on page 3-25 and the “SAF Forwarder Configuration Settings” section on page 3-26.

Hosted DN Patterns and Hosted DN Groups

- Be aware that the PSTN Failover Strip Digits, PSTN Failover Prepend Digits, and Use HostedDN as PSTN Failover settings display in both the Hosted DN Group and Hosted DN Patterns Configuration windows. If you do not configure these settings in the Hosted DN Patterns Configuration window, the Hosted DN Group configuration applies to the hosted DN patterns.
• Each hosted DN group covers one geophysical location advertising DN range.

• In the Find and List window for Hosted DN Patterns, you can download a .csv file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. Then, you can upload the patterns in the same window. (You can also add or update multiple hosted DN patterns in BAT.)

If you choose to replace the patterns when you upload the patterns, you lose all hosted DN patterns.

If invalid or bad data exists in the .csv file, the data gets ignored by Cisco Unified Communications Manager.

• Cisco Unified Communications Manager allows you to configure up to 2,000 hosted DN patterns per cluster.

• Each hosted DN pattern must be unique. Each hosted DN pattern can only exist in one hosted DN group.

• The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information on how to perform this task, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

• For information on field descriptions for hosted DN groups and hosted DN patterns, see the “Hosted DN Group Configuration Settings” section on page 3-31 and “Hosted DN Pattern Configuration Settings” section on page 3-32.

**CCD Advertising and Requesting Services**

• You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration.

• You must enable SAF on the trunk in Cisco Unified Communications Manager Administration and assign SAF-enabled trunks to the CCD advertising and requesting services in Cisco Unified Communications Manager Administration. Be aware that SAF-enabled SIP trunks only support UDP or TCP. If you want to do so, you can use the same SAF-enabled trunks for the CCD advertising service and CCD requesting service. For information on enabling SAF on the trunks, see the “Configuring a SAF-Enabled Trunk” section on page 3-45.

• You can configure one CCD requesting service. You can configure as many CCD advertising services as you want.

• Only one hosted DN group can be associated with one CCD advertising service.

• The call control discovery feature relies on a route partition, which you configure in the CCD Partition window (Call Routing > Call Control Discovery > Partition). This route partition gets used exclusively by the call control discovery to ensure that all learned patterns get placed in digit analysis under the route partition. You assign this partition to the CCD requesting service. Be aware that the CCD partition does not display under Call Routing > Class of Control > Partition in Cisco Unified Communications Manager Administration.

For field descriptions for the CCD partition, see the “Partition Configuration Settings for Call Control Discovery” section on page 3-36.

---

**Tip**

Updating the Learned Pattern Prefix field or Route Partition field in the CCD Requesting Service Configuration window may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.
• After you make changes to the configuration for the CCD advertising and requesting services, click **Save**. You do not need to click the Reset button in these windows unless you want the following events to occur:
  - For the CCD Advertising Service—The Reset button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again.
  - For the CCD Requesting Service—The Reset button in the CCD Requesting Service Configuration window causes the requesting service to remove the learned patterns from the local cache and for the requesting service to subscribe to the SAF network again. By clicking the Reset button in the CCD Requesting Service Configuration window, Cisco Unified Communications Manager can learn patterns again.

To minimize the impact to your network, Cisco recommends that you click the Reset button in the CCD Advertising Configuration window or the CCD Requesting Configuration window during off-peak hours.

Be aware that clicking Reset in the CCD Advertising and Requesting Service Configuration windows does not reset the trunk. You reset the trunk in the Trunk Configuration window.

• When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.

• When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.

• If you want a user to make outbound calls to learned patterns that are advertised by remote call-control entities, ensure that the calling search space that you assign to the device contains the route partition that is assigned to the CCD requesting service.

• When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.

• Make sure that the call-control entities do not advertise the same hosted DN patterns.

  If the call-control entities advertise the same hosted DN patterns, problems may occur; for example, a call routing loop may occur between advertising clusters when these clusters make calls to learned patterns by using a calling search space where the learned pattern partition is in front of the locally configured static partition.

• For information on field descriptions for the CCD advertising service and for the CCD requesting service, see the “CCD Advertising Service Configuration Settings” section on page 3-34 and the “CCD Requesting Service Configuration Settings” section on page 3-37.

**SAF-Enabled Trunks**

• One configured SAF-enabled H.323 trunk and one configured SAF-enabled SIP trunk can serve all SIP and H.323 calls to learned patterns for one cluster.

• Make sure that you apply the configuration to the SAF-enabled trunk before you assign the trunk to the CCD advertising or requesting service. You apply the configuration in the Trunk Configuration window.

• If you do not select/assign a SAF-enabled trunk when you configure the CCD requesting service, the CCD requesting service does not get created and patterns do not get learned.
• If you assign both a H.323 and a SIP SAF-enabled trunk to the CCD requesting service, make sure that the same Cisco Unified Communications Manager group exists in the device pool that is assigned to the trunk.

• To support clustering over WAN deployments, configure different Cisco Unified Communications Manager groups to associate with sets of SAF-enabled trunks.

• To ensure redundancy and reduce call-processing traffic, Cisco recommends that no more than two nodes exist in the Cisco Unified Communications Manager group for the device pool that you assign to the SAF-enabled trunk.

• If a trunk is assigned to a route group or associated with a route pattern, you cannot enable SAF on the trunk. Likewise, if you enable SAF on the trunk, you cannot assign the trunk to a route group or associate the trunk with a route pattern.

• Verify that the SIP trunk has a security profile of Nonsecure before you enable SAF on the trunk. You cannot enable SAF on SIP trunks that use authenticated or encrypted security profiles.

• Resetting a SAF-enabled trunk that is assigned to the CCD advertising service causes the CCD advertising service to unpublish the hosted DN patterns and republish with a different service ID for that trunk.

• If different SAF-enabled trunks are configured to use different Cisco Unified Communications Manager groups, the inbound and outbound SAF-related call traffic gets distributed among different Cisco Unified Communications Manager nodes.

• If a Cisco Unified Communications Manager group changes for the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.

• If you change the device pool of the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.

• If you want to delete a SAF-enabled trunk from Cisco Unified Communications Manager Administration, you must unassign the trunk from the CCD advertising service and/or CCD requesting service before you delete it from the Trunk Configuration window.

• Be aware that resetting a SAF-enabled trunk or changing the Cisco Unified Communications Manager group for the trunk impacts the CCD advertising and requesting services. For example, if you reset a trunk and the CCD requesting service cannot access the trunk after 10 seconds have passed, all learned patterns get purged from digit analysis and from the local cache, and the requesting process stops.

Miscellaneous Considerations

• To ensure PSTN failover, configure a route pattern and assign the route pattern to the gateway.

• If your cluster does not support E.164, you must configure translation patterns so that your users can dial E.164 numbers.
• You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

• Learned patterns are viewed in RTMT.

Call Control Discovery Feature Parameters

To access the feature parameters that support the call control discovery feature, choose Call Routing > Call Control Discovery > Feature Configuration. Table 3-5 describes the feature parameters for the call control discovery feature. For additional information, you can click the question mark help in the Feature Configuration window.

Table 3-5  Call Control Discovery Feature Parameters

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD Maximum Number of Learned Patterns</td>
<td>This parameter specifies the number of patterns that this Cisco Unified Communications Manager cluster can learn from the SAF network. The higher the number of allowed learned patterns, the more memory and CPU processing power is required for your server. When Cisco Unified Communications Manager attempts to learn more patterns than is specified in the parameter configuration, the alarm, CDLLearnedPatternLimitReached, gets issued. You can enter a number from 1 to 20000, which is the default.</td>
</tr>
<tr>
<td>CCD Learned Pattern IP Reachable Duration</td>
<td>This parameter specifies the number of seconds that learned patterns stay active (reachable) before Cisco Unified Communications Manager marks those patterns as unreachable. For example, you configure 20 seconds for this parameter; when Cisco Unified Communications Manager cannot communicate with the SAF forwarder after 20 seconds, all calls to learned patterns fail over to the PSTN until IP connectivity to the SAF forwarder gets restored. During the PSTN failover, Cisco Unified Communications Manager cannot learn new patterns. After the time that you specified for this parameter elapses, Cisco Unified Communications Manager marks the learned patterns as unreachable. Use this parameter with the CCD PSTN Failover Duration parameter, which allows patterns that have been marked as unreachable to be reached through PSTN failover. You can enter a number (seconds) from 0 to 300; the default equals 60 seconds.</td>
</tr>
</tbody>
</table>
### Table 3-5 Call Control Discovery Feature Parameters (continued)

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD PSTN Failover Duration</td>
<td>This parameter specifies the number of minutes that calls to unreachable/inactive learned patterns are routed through the PSTN gateway and then purged from the system. The configuration for this parameter does not take effect until after the timer expires for the CCD Learned Pattern IP Reachable Duration parameter. The expiration of the CCD Learned Pattern IP Reachable Duration parameter indicates that IP connectivity fails between the SAF forwarder and Cisco Unified Communications Manager, and all learned patterns get marked as unreachable. Then, when the duration expires for CCD PSTN Failover Duration parameter, all learned patterns get purged from the system and calls to purged patterns are rejected (caller hears reorder tone or “number is unavailable” announcement). Setting this parameter to 0 means that PSTN failover cannot occur; that is, if the SAF forwarder cannot be reached for the number of seconds that you defined in the CCD Learned Pattern IP Reachable Duration parameter, no failover option is provided over the PSTN, and calls to learned patterns immediately fail. Setting this parameter to 525600 means that PSTN failover never expires and learned patterns never get purged because of IP connectivity issues. You can enter a number (minutes) from 0 to 525600; the default equals 2880.</td>
</tr>
<tr>
<td>Issue Alarm for Duplicate Learned Patterns</td>
<td>This parameter determines whether Cisco Unified Communications Manager issues the alarm, DuplicateLearnedPattern, when it learns duplicate patterns from different remote call-control entities on the SAF network. The default equals False.</td>
</tr>
</tbody>
</table>
Table 3-5   Call Control Discovery Feature Parameters (continued)

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD Stop Routing On Unallocated Unassigned Number</td>
<td>This parameter determines whether Cisco Unified Communications Manager continues to route calls to a remote call-control entity, such as a Cisco Unified Communications Manager cluster or Cisco Unified Communications Manager Express, when the remote call-control entity rejects the call with the cause code for Unallocated/Unassigned Number. Be aware that an unallocated number represents a hosted DN that does not exist in the current call control entity. The default equals True. If the parameter is set to True, the call is released as soon as Cisco Unified Communications Manager receives the cause code from the remote call-control entity. If the parameter is set to False, when Cisco Unified Communications Manager extends the call to the learned pattern and the remote call-control entity sends the unallocated number cause value, Cisco Unified Communications Manager attempts to find another reachable IP address for the remote cluster for this learned pattern. If any reachable remote destination is available, Cisco Unified Communications Manager tries to extend the call to the IP address of the available reachable remote cluster.</td>
</tr>
</tbody>
</table>

SAF Security Profile Configuration Settings

Configuration Path—Advanced Features > SAF > SAF Security Profile

In the SAF Security Profile Configuration window, you configure a SAF security profile so that a secure connection occurs between the SAF forwarder and the Cisco Unified Communications Manager. When you configure a SAF forwarder in the SAF Forwarder Configuration window, you must choose a SAF security profile to apply to the SAF forwarder.

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. For more information on the call control discovery feature, see the “Call Control Discovery” section on page 3-1.

Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder.

Before You Begin

Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.

Before you configure the SAF security profile, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.
Table 3-6  SAF Security Profile Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the SAF security profile. The name that you enter displays in the Find and List SAF Security Profile window and in the SAF Security Profile drop-down list box in the SAF Forwarder Configuration window. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank spaces. You can configure up to 50 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the SAF security profile. You can enter all characters except for , “, &lt;, &gt;, &amp; and %. You can configure up to 128 characters.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder. Tip To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same user name that you entered on the router (SAF forwarder). The user name is case sensitive, so enter the user name exactly as you entered it on the SAF forwarder. The value that you enter represents the shared secret for message integrity checks between Cisco Unified Communications Manager and the SAF forwarder. The user name gets included in any request from Cisco Unified Communications Manager that contains the MESSAGE-INTEGRITY attribute.</td>
</tr>
<tr>
<td>User Password</td>
<td>Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder. Tip To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same password that you entered on the router (SAF forwarder). The password is case sensitive, so enter the password exactly as you entered it on the SAF forwarder.</td>
</tr>
</tbody>
</table>

SAF Forwarder Configuration Settings

Configuration Path—Advanced Features > SAF > SAF Forwarder
A SAF forwarder, a Cisco router that you configure for call control discovery/SAF, handles the publishing requests from Cisco Unified Communications Manager for the call control discovery feature. In addition, the SAF forwarder handles advertising requests from remote call-control entities for the call control discovery feature. For information on call control discovery, see the “Call Control Discovery” section on page 3-1.

Before You Begin
Before you configure the SAF forwarder, make sure that you have configured at least one SAF security profile.

Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.

Before you configure the SAF forwarder, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-7 SAF Forwarder Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the SAF forwarder. Valid entries include alphanumeric characters, hyphen, period, and underscore. You can enter up to 50 characters. The value that you enter in this field gets used to classify SAF forwarder records in the database. The value that you enter displays in the Find and List SAF Forwarder window when you perform a search.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the SAF forwarder. You can enter all characters except for , ‘“, &lt; , &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>
Configuring Call Control Discovery

Client Label

The client label allows the SAF forwarder to identify the Cisco Unified Communications Manager node. Valid entries include alphanumeric characters, underscore, and @. You can enter up to 50 characters.

Each Cisco Unified Communications Manager node that you select to interact with this SAF forwarder includes its unique client label in the registration message that it sends to the SAF forwarder. When the SAF forwarder receives the registration message, it verifies whether you configured the client label on the SAF forwarder.

When you configure a single SAF forwarder for the entire cluster, all nodes in the cluster use the same SAF forwarder configuration and register to the same SAF forwarder. To create a unique client label for the nodes in the cluster, you can append @ to the client label value, which ensures that the registration message includes the basename followed by @<nodeid>. For example, you enter abcde_ny@ for the client label for a two-node cluster that connects to one SAF forwarder, so the registration message includes abcde_ny@1 for node 1 or abcde_ny@2 for node 2.

If you do not append the @ to the client label value, you do not need to configure the basename parameter for the client label on the router, but you do need to configure the client label on the router. If you append the @ to the client label value, you must configure the basename parameter with the client label on the router.

Tip

If more than one Cisco Unified Communications Manager node displays in the Selected Cisco Unified Communications Managers pane under the Showed Advanced section, append @ to the client label value; otherwise, errors may occur because each node uses the same client label to register with the SAF forwarder.

Table 3-7 SAF Forwarder Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Label</td>
<td>The client label allows the SAF forwarder to identify the Cisco Unified Communications Manager node. Valid entries include alphanumeric characters, underscore, and @. You can enter up to 50 characters. Each Cisco Unified Communications Manager node that you select to interact with this SAF forwarder includes its unique client label in the registration message that it sends to the SAF forwarder. When the SAF forwarder receives the registration message, it verifies whether you configured the client label on the SAF forwarder. When you configure a single SAF forwarder for the entire cluster, all nodes in the cluster use the same SAF forwarder configuration and register to the same SAF forwarder. To create a unique client label for the nodes in the cluster, you can append @ to the client label value, which ensures that the registration message includes the basename followed by @&lt;nodeid&gt;. For example, you enter abcde_ny@ for the client label for a two-node cluster that connects to one SAF forwarder, so the registration message includes abcde_ny@1 for node 1 or abcde_ny@2 for node 2. If you do not append the @ to the client label value, you do not need to configure the basename parameter for the client label on the router, but you do need to configure the client label on the router. If you append the @ to the client label value, you must configure the basename parameter with the client label on the router.</td>
</tr>
</tbody>
</table>
Table 3-7 SAF Forwarder Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF Security Profile</td>
<td>Choose the SAF security profile that you want to apply to this SAF forwarder. The username and password from the security profile get sent to the SAF forwarder, so choose a security profile that contains a username and password that the SAF forwarder will accept. (The SAF forwarder must be configured to use the same username and password.)</td>
</tr>
<tr>
<td>SAF Forwarder Address</td>
<td>Enter the IPv4 address of the SAF forwarder.</td>
</tr>
<tr>
<td>SAF Forwarder Port</td>
<td>Enter the port number that Cisco Unified Communications Manager uses to establish a connection with the SAF forwarder. The default setting is 5050. The port that you enter must match the port number that you configure on the SAF forwarder. The port range on the SAF forwarder is 1024 to 65535.</td>
</tr>
<tr>
<td>Enable TCP Keep Alive</td>
<td>Check the Enable TCP Keep Alive check box to ensure that Cisco Unified Communications Manager gets notified if the TCP connection between the SAF forwarder and Cisco Unified Communications Manager fails. If this check box is unchecked, the Cisco Unified Communications Manager does not get notified that the TCP connection fails until the SAF forwarder keepalive timer expires (configured on the SAF forwarder). Cisco recommends that this check box remains checked.</td>
</tr>
<tr>
<td>Show/Hide Advanced</td>
<td></td>
</tr>
<tr>
<td>SAF Reconnect Interval</td>
<td>Enter the time (in seconds) that Cisco Unified Communications Manager allows to pass before it attempts to reconnect to the SAF forwarder after a connection failure. Enter a value between 0 and 500. The default value is 20.</td>
</tr>
<tr>
<td>SAF Notifications Window Size</td>
<td>Enter the number of outstanding Notify requests that the SAF forwarder can maintain at the same time to the Cisco Unified Communications Manager. The default value is 7. You can enter a number between 0 to 255. If you enter 0 in this field, the SAF forwarder does not send any notification to this Cisco Unified Communications Manager, but the Cisco Unified Communications Manager can still publish hosted DNs to the SAF network if the CCD advertising service is configured and active.</td>
</tr>
</tbody>
</table>
### Selected Cisco Unified Communications Managers

Use this pane for cluster over WAN (COW) configurations.

This pane displays the nodes that prioritize this SAF forwarder over other configured SAF forwarders. For example, if node_1 and node_2 display in this pane for forwarder1, then node_1 and node_2 always choose forwarder1 first, even though you may have configured other SAF forwarders.

To move a node to or from the Selected Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow below the Available Cisco Unified Communications Managers pane. Highlight the nodes in the pane, click the up or down arrow to the right of the pane.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Cisco Unified Communications Managers</td>
<td>This setting works with the Selected Cisco Unified Communications Managers pane. Every node in the Available Cisco Unified Communications Managers pane can connect to the SAF forwarder that you configure in the SAF Forwarder Configuration window. If you want to do so, you can assign a particular node to this SAF forwarder so that the node prioritizes this SAF forwarder over other configured SAF forwarders. You assign the node to the SAF forwarder by moving the node to the Selected Cisco Unified Communications Managers pane. To move a node to or from the Available Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow. If you have assigned a node to two SAF forwarders, the assigned node does not display in the pane because you can only assign a node to two SAF forwarders. For example, three SAF forwarders exist—forwarder1, forwarder2, and forwarder3. You assign node_2 to forwarder1 and forwarder3, which means that node_2 does not display in the Available Cisco Unified Communications Managers pane for forwarder2.</td>
</tr>
<tr>
<td>Selected Cisco Unified Communications Managers</td>
<td>Use this pane for cluster over WAN (COW) configurations. This pane displays the nodes that prioritize this SAF forwarder over other configured SAF forwarders. For example, if node_1 and node_2 display in this pane for forwarder1, then node_1 and node_2 always choose forwarder1 first, even though you may have configured other SAF forwarders. To move a node to or from the Selected Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow below the Available Cisco Unified Communications Managers pane. Highlight the nodes in the pane, click the up or down arrow to the right of the pane.</td>
</tr>
</tbody>
</table>
Hosted DN Group Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Hosted DN Group

Supported with the call control discovery feature, hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. After you assign a hosted DN group to the CCD advertising service in Cisco Unified Communications Manager Administration, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD Advertising Service.

For more information on the call control discovery feature, see the “Call Control Discovery” section on page 3-1.

Before You Begin

Before you configure the hosted DN groups, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-8 Hosted DN Group Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the hosted DN group. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. The value that you enter displays in the Find and List Hosted DN Group window, the Hosted DN Group Configuration window, the Hosted DN Pattern Configuration window, and the CCD Advertising Service Configuration window,</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the hosted DN group. You can enter all characters except for , &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>PSTN Failover Strip Digits</td>
<td>Enter the number of digits that you want stripped from the hosted DN if the call fails over to the PSTN. You can enter a value between 0 and 16.</td>
</tr>
<tr>
<td>PSTN Failover Prepend Digits</td>
<td>Enter the international escape character, +, or digits (0-9) that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. For example, enter an access or area code.</td>
</tr>
</tbody>
</table>
Hosted DN Pattern Configuration Settings

Configuration Path—**Call Routing > Call Control Discovery > Hosted DN Patterns**

Hosted DN Pattern Configuration window supports the call control discovery feature, which allows Cisco Unified Communications Manager to use the SAF network to learn information, such as directory number patterns, from other remote call-control entities that also advertise SAF.

Hosted DN patterns are directory number patterns that belong to Cisco Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns with Hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.

**Table 3-9** describes the configuration settings that display in the Hosted DN Pattern Configuration window; these same settings display in the .csv file where you can add or modify hosted DN patterns and then upload them into the Cisco Unified Communications Manager database.

**Before You Begin**

Before you configure the hosted DN patterns, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

For more information on call control discovery, see the “Call Control Discovery” section on page 3-1.
### Table 3-9 Hosted DN Pattern Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted Pattern</td>
<td>Enter the value for the hosted DN pattern, which can contain a maximum of 50 characters. The value that you enter in this field gets advertised by the CCD advertising service to remote call-control entities. You can enter the international escape character + followed by pattern or dialable digits (0-9A-Da-d), pattern ([6-9]), wildcard character (X), or (^) with optional % or ! at the end of the entry.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the hosted DN pattern. You can enter all characters except for , &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>
| Hosted DN Group           | Choose the Hosted DN group that you want to associate with this hosted DN pattern. If both of the following conditions are met, Cisco Unified Communications Manager applies the PSTN failover configuration for the hosted DN group to the hosted DN pattern:  
  - In the Hosted DN Patterns window, you do not configure the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields (or you use the defaults).  
  - In the Hosted DN Patterns window, you uncheck the Use HostedDN as PSTN Failover check box. |
| PSTN Failover Strip Digits| Enter the number of digits that you want to strip from the beginning of the directory number when an IP connection is not available and the call fails over to the PSTN. You can enter a value between 0 and 16.  
When all of the following conditions are met, the hosted DN group configuration applies:  
  - When you enter 0 in this field (or leave it blank)  
  - When you leave the PSTN Failover Prepend Digits field blank  
  - When the Use Hosted DN as PSTN Failover check box is unchecked  
If the value that you enter in this field is longer than the hosted DN pattern, all digits in the pattern get stripped before any digits are prepended. |
Configuring Call Control Discovery

Before You Begin
Before you configure the CCD advertising service, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-9 Hosted DN Pattern Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| PSTN Failover Prepend Digits  | Enter the international escape character, +, or the digits that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. When all of the following conditions are met, the hosted DN group configuration applies:  
  • When you enter 0 in this field (or leave it blank)  
  • When you leave the PSTN Failover Strip Digits field blank  
  • When the Use Hosted DN or PSTN Failover check box is unchecked |
| Use HostedDN as PSTN Failover | If you do not need to strip digits from or prepend digits to the hosted DN when the call fails over to the PSTN, check the **Use Hosted DN as PSTN Failover** check box. When you check the check box, the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields display as disabled. If you check the check box, the entity that makes the outbound call uses the original hosted DN range for PSTN failover. If you are modifying the .csv file for hosted DN patterns, enter **TRUE**, which indicates that you want to use the Hosted DN exactly as is during PSTN failover, or **FALSE**, which indicates that you plan to strip digits from and prepend digits to the directory number during PSTN failover. |

**CCD Advertising Service Configuration Settings**

Configuration Path—Call Routing > Call Control Discovery > Advertising Service

The call control discovery advertising service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network. Table 3-10 describes the CCD Advertising Service configurations settings.
### Configuring Call Control Discovery

#### Additional Information
See the “Related Topics” section on page 3-47.

#### Table 3-10 CCD Advertising Service Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the CCD advertising service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the CCD advertising service. You can enter all characters except for , &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>SAF SIP Trunk</td>
<td>Choose the SIP trunk that you want to use with this CCD advertising service. For inbound calls to the Cisco Unified Communications Manager, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, you did not choose Call Control Discovery from the Trunk Service Type drop-down list box when you first configured the trunk.</td>
</tr>
<tr>
<td>SAF H323 Trunk</td>
<td>Choose the H.323 trunk that you want to use with the CCD advertising service. For inbound calls to the Cisco Unified Communications Manager, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, verify that you checked the Enable SAF check box in the Trunk Configuration window for H.323 (non-gatekeeper controlled) trunks.</td>
</tr>
<tr>
<td>HostedDN Group</td>
<td>Choose the Hosted DN group that you want to associate with this CCD advertising service. The CCD advertising service advertises the hosted DN patterns that are a part of the hosted DN group. You can only assign the hosted DN group to one CCD advertising service, so only unassigned hosted DN groups display in this drop-down list box.</td>
</tr>
<tr>
<td>Activated Feature</td>
<td>Ensure the Activated Feature check box is checked. If the Activated Feature check box is not checked, the CCD advertising service does not work.</td>
</tr>
</tbody>
</table>
Partition Configuration Settings for Call Control Discovery

Configuration Path—Call Routing > Call Control Discovery > Partition

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis master routing table.

The partition under Call Routing > Call Control Discovery > Partition only supports the call control discovery feature; that is, all learned patterns automatically belong to the CCD partition that you assign to the CCD requesting service. The call control discovery partition ensures that the learned patterns get inserted into digit analysis under this partition for call control discovery.

Be aware that the CCD partition does not display under Call Routing > Class of Control > Partition in Cisco Unified Communications Manager Administration.

Before You Begin

Before you configure the CCD partition, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Next Steps

Assign the partition to the CCD requesting service.

The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

Table 3-11 Partition Configuration Settings for Call Control Discovery

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the partition that you plan to assign to the CCD requesting service. You can enter alphanumeric characters, underscore (_), hyphen (-), or space. You can enter up to 50 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the partition. You can enter all characters except for &quot;, &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>
Configuring Call Control Discovery

CCD Requesting Service Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Requesting Service

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis.

In Cisco Unified Communications Manager Administration, you can configure only one call control discovery requesting service.

Table 3-11  Partition Configuration Settings for Call Control Discovery (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Time Schedule | From the drop-down list box, choose a time schedule to associate with this CCD partition. The associated time schedule specifies when the partition is available to make outgoing calls to learned patterns for this cluster.  
The default value specifies None, which implies that time-of-day routing is not in effect and the partition remains active at all times.  
In combination with the Time Zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks outgoing calls to learned patterns under this partition against the specified time schedule. |
| Time Zone    | Choose one of the following options to associate a CCD partition with a time zone:  
  • Originating Device—If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device.  
  • Specific Time Zone—If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone.  
  When an outgoing call to a CCD learned pattern occurs, the current time on the Cisco Unified Communications Manager gets converted into the specific time zone set when one option is chosen. The system validates this specific time against the value in the Time Schedule field. |
### Before You Begin

Before you configure the CCD requesting service, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

### Table 3-12  CCD Requesting Service Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the CCD requesting service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the CCD requesting service. You can enter all characters except for , “, &lt;, &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>From the drop-down list box, choose the partition where you want the learned patterns to belong. The Route Partition field only supports the call control discovery feature; that is, all learned patterns automatically belong to the partition that you choose. This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition. If you choose a partition besides None from the drop-down list box, the partition that you choose must belong to a calling search space that the devices can use for calling the learned patterns. In this case, if you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.</td>
</tr>
</tbody>
</table>

**Tip**  
Cisco strongly recommends that you configure a unique partition and assign it to the CCD requesting service. If you choose None from the Route Partition drop-down list box, all devices can call the learned patterns.

**Tip**  
Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.
Chapter 3      Call Control Discovery

Table 3-12      CCD Requesting Service Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learned Pattern Prefix</td>
<td>The learned pattern prefix gets applied to the hosted DN pattern before the CCD requesting service registers with digit analysis. For outgoing calls to learned patterns, the learned pattern prefix gets stripped. Enter the prefix that you want to apply to the hosted DN pattern before the hosted DN pattern registers with digit analysis. To make calls to the learned patterns, the phone user must dial the prefix followed by the learned pattern. You can enter numbers, *, #, or +. You can enter up to 24 characters. <strong>Tip</strong> Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.</td>
</tr>
<tr>
<td>PSTN Prefix</td>
<td>Enter the digits that will get prepended to the learned patterns when PSTN failover occurs. You can enter numbers, *, #, or +. You can enter up to 24 characters. When calls to learned patterns fail over to the PSTN, the PSTN prefix gets added to the learned pattern after the PSTN failover settings that are advertised by the remote call-control entity for that learned pattern get applied.</td>
</tr>
<tr>
<td>Available SAF Trunks</td>
<td>A list of SAF-enabled trunks that are not assigned to the CCD requesting service display in the Available SAF Trunks pane. To assign the trunk to the CCD requesting service, highlight the service and click the down arrow to move the trunk to the Selected SAF Trunks pane.</td>
</tr>
<tr>
<td>Selected SAF Trunks</td>
<td>Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns. A list of SAF-enabled trunks that are assigned to the CCD requesting service display in the Selected SAF Trunks pane. You can assign as many SAF-enabled trunks as you want. Outbound calls get managed in a round-robin fashion; that is, if the learned pattern supports both SIP and H.323 protocol, then outbound calls alternate between the trunk types. To unassign the trunk from the CCD requesting service, highlight the service and click the up arrow to move the trunk to the Available SAF Trunks pane. To order the trunks in the pane, highlight the trunk and click the up and down arrows to the right of the pane. <strong>Tip</strong> At least one SAF-enabled trunk must exist in the Selected SAF Trunks pane; otherwise, the CCD requesting service does not get started for the local cluster, and patterns do not get learned.</td>
</tr>
</tbody>
</table>
Blocked Learned Pattern Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Blocked Learned Patterns

The Blocked Learned Pattern Configuration window supports the call control discovery feature by allowing you to purge and block learned patterns, for example, learned patterns that you no longer want to use.

If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from remote call-control entity, xyz with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from remote call-control entity xyz with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity and IP address for the entity, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that use it.

Tip
You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network and if the maximum number of learned patterns has not been reached for the cluster. For a pattern to be relearned by Cisco Unified Communications Manager, you must delete the entire record for the blocked learned pattern from Cisco Unified Communications Manager Administration; that is, Cisco Unified Communications Manager does not relearn a pattern when you only delete part of the blocked learned pattern configuration; for example, if you only delete the Remote Call Control Identity or Remote IP configuration for the record.

For Cisco Unified Communications Manager to block or purge a pattern, the learned pattern must match all data that you configure in the Blocked Learned Patterns window.
Table 3-13 describes the blocked learned patterns configuration settings that display in the Blocked Learned Pattern Configuration window.

**Table 3-13  Blocked Learned Pattern Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Learned Pattern      | **Tip** If you want Cisco Unified Communications Manager to block all patterns based on a prefix that gets prepended to the directory number, do not configure this field; instead, configure the Learned Pattern Prefix field.  
**Tip** If you want to block all learned patterns from a particular remote call-control entity, do not configure this field; instead, configure the Remote Call Control Identity field or the Remote IP field.  
For this field, enter the exact learned pattern that you want to block. Cisco Unified Communications Manager blocks a pattern based on exact match, so you must enter the exact pattern that you want Cisco Unified Communications Manager to block. For example, if you enter 235XX, Cisco Unified Communications Manager blocks 235XX patterns. |
| Learned Pattern Prefix | **Tip** If you configured the Learned Pattern field, do not configure the Learned Pattern Prefix field.  
If you want to block a learned pattern based on the prefix that is prepended to the pattern, enter the prefix in this field. For example, if you want to block learned patterns that use +1, enter +1 in this field.  
If you configure the Remote Call Control Identity or Remote IP fields, Cisco Unified Communications Manager blocks the learned patterns that use the particular prefix from the remote call-control entity that you configure (not from all remote call-control entities that advertise patterns with the prefix). If you do not enter a remote call-control entity or remote IP address, then all patterns that use the prefix get blocked. |
| Remote Call Control Identity | Enter the name of the remote call-control entity that advertises the pattern that you want to block. For example, you may enter the name of a cluster or a site.  
If you leave this field and the Remote IP field blank, Cisco Unified Communications Manager blocks the learned pattern for all remote call-control entities that advertise the pattern. |
| Remote IP             | Enter the IP address for the remote call-control entity where you want to block the learned pattern.  
If you want to block a particular learned pattern from all remote call-control entities, you do not need to configure this field. Configure this field when you want to block a particular learned pattern from a specific remote call-control entity. |
Finding Configuration Records for Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

After you configure call control discovery, you can search for the configuration records in the related Find and List windows in Cisco Unified Communications Manager Administration. The Find and List windows allow you to search for records based on specific criteria.

**Note**

During your work in a browser session, Cisco Unified Communications Manager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your search preferences until you modify your search or close the browser.

**Procedure**

**Step 1** To locate one of the Find and List windows for the call control discovery feature in Cisco Unified Communications Manager Administration, perform one of the following tasks:

- Choose Advanced Features > SAF > SAF Security Profile.
- Choose Advanced Features > SAF > SAF Forwarder.
- Choose Call Routing > Call Control Discovery > Hosted DN Group.
- Choose Call Routing > Call Control Discovery > Hosted DN Patterns.
- Choose Call Routing > Call Control Discovery > Advertising Service.
- Choose Call Routing > Call Control Discovery > Partition.
- Choose Call Routing > Call Control Discovery > Blocked Learned Pattern.

**Tip**

No Find and List window displays for the CCD requesting service because you can configure only one CCD requesting service in Cisco Unified Communications Manager Administration. When you choose Call Routing > Call Control Discovery > Requesting Service, the record, if configured, displays.

In the Find and List window for Hosted DN Patterns, you can download a .csv file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. To download a .csv file, click Download in the window. To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click Upload File; browse to the file that you
want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click Upload File.

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

The Find and List window displays. Records from an active (prior) query may also display in the window.

**Step 2**

To find all records in the database, ensure the dialog box is empty; go to **Step 3**.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

**Note**

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

If you search by the search parameter, Activated Feature, in the Find and List CCD Advertising Service window, you must enter t or f to indicate true or false if you specify search text. Do not enter true or false when you specify the search text.

**Step 3**

Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Note**

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configured records for this selection by clicking Select All and then clicking Delete Selected.

**Step 4**

From the list of records that display, click the link for the record that you want to view.

**Note**

To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

**Additional Information**

See the “Related Topics” section on page 3-47.
### Configuring Call Control Discovery (Procedure)

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

This section describes how to add, copy, or update configuration for call control discovery in the Cisco Unified Communications Manager database. For call control discovery, you configure a SAF security profile, SAF forwarders, hosted DN groups and patterns, CCD advertising services, and the CCD requesting service. Before you configure call control discovery, see the “Configuration Checklist for Call Control Discovery” section on page 3-2.

---

**Tip**

This section does not describe how to enable trunks for SAF. For information on how to enable a trunk for SAF, see the “Hosted DN Group Configuration Settings” section on page 3-31.

To identify which hosted DN patterns belong to a hosted DN group, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

This section does not display how to access the CCD Feature Configuration window, which displays feature parameters for call control discovery. For more information on feature parameters, see the “Call Control Discovery Feature Parameters” section on page 3-23.

---

**Procedure**

**Step 1**
Perform one of the following tasks:

- If you are configuring the CCD requesting service, choose Call Routing > Call Control Discovery > Requesting Service. The CCD Requesting Service Configuration window displays; go to Step 3.
- Choose Advanced Features > SAF > SAF Security Profile.
- Choose Advanced Features > SAF > SAF Forwarder.
- Choose Call Routing > Call Control Discovery > Hosted DN Group.
- Choose Call Routing > Call Control Discovery > Hosted DN Patterns.
- Choose Call Routing > Call Control Discovery > Advertising Service.
- Choose Call Routing > Call Control Discovery > Blocked Learned Pattern.

The Find and List window displays for the SAF Security Profile, SAF Forwarder, Hosted DN Group, Hosted DN Patterns, Partition, and CCD Advertising Service windows.

**Step 2**
From the Find and List window, perform one of the following tasks:

- To copy an existing record related to call control discovery, locate the record as described in the “SAF Security Profile Configuration Settings” section on page 3-25, click the Copy button next to the record that you want to copy, and continue with Step 3.
- To add a new record related to call control discovery, click the Add New button and continue with Step 3.
To update an existing record, locate the appropriate record as described in the “SAF Security Profile Configuration Settings” section on page 3-25 and continue with Step 3.

In the Find and List window for Hosted DN Patterns, you can download a .csvs file so that you can add or update multiple patterns for the call control discovery feature at the same time. To download a .csv file, click Download in the window.

**Step 3** Configure the appropriate fields as described in the following sections:
- SAF Security Profile Configuration Settings, page 3-25
- SAF Forwarder Configuration Settings, page 3-26
- Hosted DN Group Configuration Settings, page 3-31
- Hosted DN Pattern Configuration Settings, page 3-32
- Partition Configuration Settings for Call Control Discovery, page 3-36
- CCD Advertising Service Configuration Settings, page 3-34
- CCD Requesting Service Configuration Settings, page 3-37
- Blocked Learned Pattern Configuration Settings, page 3-40

**Step 4** To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click Upload File; browse to the file that you want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click Upload File.

**Step 5** To save the configuration information to the database, click Save.

**Tip** The Reset button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again. The Reset button in the CCD Requesting Service Configuration window triggers the requesting service to remove the learned patterns from the local cache, resubscribe to the SAF network, and to learn patterns again. To ensure that your network is not impacted, Cisco recommends that you click the Reset button during off-peak hours.

**Additional Information**
See the “Related Topics” section on page 3-47.

**Configuring a SAF-Enabled Trunk**

You can configure a SIP or H.323 (non-gatekeeper controlled) trunk so that it supports SAF. For SIP trunks, you choose Call Control Discovery from the Trunk Service Type drop-down list box, which displays in the same window where you assign the trunk type and trunk protocol. Be aware that you cannot change the trunk service type after you choose it from the drop-down list box.

For H.323 (non-gatekeeper controlled) trunks, you check the Enable SAF check box in the Trunk Configuration window when you configure the trunk (after you choose the trunk type and trunk protocol). If you want to disable SAF on the H.323 trunk after you enable it, uncheck the Enable SAF check box.

For trunk configuration considerations, see the “Considerations for Call Control Discovery Configuration” section on page 3-19.
Identifying Which Hosted DN Patterns Belong to a Hosted DN Group

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. In the Find and List Hosted DN Patterns window, you can perform one of the following tasks:

- You can search for all hosted DN patterns, which displays the hosted DN group in the Hosted DN Group when the results display. (The GUI groups the hosted DN groups together in the results.)
- You can search specifically for a particular hosted DN group by choosing Hosted DN Group from the Find drop-down list box and then entering a hosted DN group in the search criteria.

Deleting Configuration Records for Call Control Discovery

This section describes how to delete a configured call control discovery record in Cisco Unified Communications Manager Administration.

Before You Begin

If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.

When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.

Note

You can delete multiple records from the Find and List window by checking the check boxes next to the appropriate records and clicking **Delete Selected**. You can delete all records in the window by clicking **Select All** and then clicking **Delete Selected**.

Procedure

**Step 1**

If you want to delete the record from the Find and List window, perform the following tasks:

a. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for Call Control Discovery” section on page 3-42.

b. Click the record that you want to delete.

c. Click **Delete Selected**.

You receive a message that asks you to confirm the deletion.

d. Click **OK**.

The window refreshes, and the record gets deleted from the database.

**Step 2**

If you want to delete the record from the configuration window, perform the following tasks:

a. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for Call Control Discovery” section on page 3-42.

b. Access the configuration window; click **Delete** in the configuration window.

You receive a message that asks you to confirm the deletion.
c. Click OK.

The window refreshes, and the record gets deleted from the database.

Additional Information
See the “Related Topics” section on page 3-47.

Providing Information to End Users

The call control discovery feature does not impact end users; for example, it does not impact phone users.

Troubleshooting Call Control Discovery

For information on troubleshooting call control discovery, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Related Topics

- Configuration Checklist for Call Control Discovery, page 3-2
- Introducing Call Control Discovery for Cisco Unified Communications Manager, page 3-5
  - Overview of Call Control Discovery, page 3-5
  - Components for the Call Control Discovery Feature, page 3-6
- System Requirements for Call Control Discovery, page 3-16
- Interactions and Restrictions, page 3-16
- Installing and Activating Call Control Discovery, page 3-18
- Configuring Call Control Discovery, page 3-18
  - Considerations for Call Control Discovery Configuration, page 3-19
  - Call Control Discovery Feature Parameters, page 3-23
  - SAF Security Profile Configuration Settings, page 3-25
  - SAF Forwarder Configuration Settings, page 3-26
  - Hosted DN Group Configuration Settings, page 3-31
  - Hosted DN Pattern Configuration Settings, page 3-32
  - CCD Advertising Service Configuration Settings, page 3-34
  - Partition Configuration Settings for Call Control Discovery, page 3-36
  - CCD Requesting Service Configuration Settings, page 3-37
  - Blocked Learned Pattern Configuration Settings, page 3-40
  - Finding Configuration Records for Call Control Discovery, page 3-42
  - SAF Security Profile Configuration Settings, page 3-25
Related Topics

- Configuring a SAF-Enabled Trunk, page 3-45
- Identifying Which Hosted DN Patterns Belong to a Hosted DN Group, page 3-46
- Deleting Configuration Records for Call Control Discovery, page 3-46
- Providing Information to End Users, page 3-47
- Troubleshooting Call Control Discovery, page 3-47
- *Cisco IOS Service Advertisement Framework Configuration Guide*
- *Cisco IOS Service Advertisement Framework Command Reference*
Call Display Restrictions

The Call Display Restrictions feature allows you to choose the information that will display for calling and/or connected lines, depending on the parties who are involved in the call. By using specific configuration settings in Cisco Unified Communications Manager Administration, you can choose to present or restrict the display information for each call.

For example, in a hotel environment, you may want to see the display information for calls that are made between a guest room and the front desk; however, for calls between guest rooms, you would not want the call information to display on either phone. The Call Display Restrictions feature enables this functionality.

This chapter provides the following information about using the Call Display Restrictions feature in Cisco Unified Communications Manager:

- Configuration Checklist for Call Display Restrictions, page 4-1
- Introducing Call Display Restrictions, page 4-2
- System Requirements for Call Display Restrictions, page 4-4
- Scenarios for Using Call Display Restrictions, page 4-4
- Interactions, page 4-5
- Configuring Call Display Restrictions, page 4-6
- Related Topics, page 4-14

Configuration Checklist for Call Display Restrictions

The Call Display Restrictions feature allows you to choose the information that will display for calling and/or connected lines, depending on the parties who are involved in the call. By using specific configuration settings in Cisco Unified Communications Manager Administration, you can choose to present or restrict the display information for each call.

For example, in a hotel environment, you may want to see the display information for calls that are made between a guest room and the front desk; however, for calls between guest rooms, you would not want the call information to display on either phone. The Call Display Restrictions feature enables this functionality.
Table 4-1 provides a checklist to configure Call Display Restrictions. For more information on Call Display Restrictions, see the “Introducing Call Display Restrictions” section on page 4-2 and the “Related Topics” section on page 4-14.

### Table 4-1  Call Display Restrictions Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure partitions for rooms, front desk, club, and the PSTN. See the “Partitions” section on page 4-9.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure call park directory numbers or define a range of call park directory numbers. Configure translation patterns for each call park directory number for call park retrieval from rooms. See the “Call Park” section on page 4-13.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure a partition for call park directory numbers to make the partition available only to users who have the partition in their calling search space. See the “Partitions” section on page 4-9 and the “Call Park” section on page 4-13.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure calling search spaces for rooms, front desk, club, the PSTN, and room park range (for Call Park). See the “Calling Search Spaces” section on page 4-10.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure the phones for the rooms, front desk, club, and the gateway for the PSTN. See the “Devices and Gateways” section on page 4-10.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configure translation patterns and route patterns. See the “Translation Patterns” section on page 4-11.</td>
</tr>
</tbody>
</table>

### Introducing Call Display Restrictions

The Call Display Restrictions feature works within a Cisco Unified Communications Manager cluster that is running Cisco Unified Communications Manager 5.0 or a later version. To enable Call Display Restrictions, you must configure the following parameters:

**Service Parameter:**
- Always Display Original Dialed Number

**Translation Pattern Parameters**
- Calling Line ID Presentation
- Connected Line ID Presentation
Chapter 4  Call Display Restrictions

Introducing Call Display Restrictions

Phone Configuration/User Device Profile Parameter:

- Ignore Presentation Indicators (internal calls only)

The combination of these settings allows you to determine whether the display information for each call is allowed or restricted and how to display the connected number.

This section includes the following topics:

- Overview of Call Display Restrictions, page 4-3
- Enabling Call Display Restrictions, page 4-3

Overview of Call Display Restrictions

Call Display Restrictions allow you to selectively display or restrict calling and/or connected line display information. A hotel environment, which might have the following needs, frequently requires this functionality:

- For calls between a guest room and the front desk, both the room and the front desk should see the call information display of each other.
- For calls between guest rooms, the rooms should not see the call information display of each other.
- For calls between guest rooms and other hotel extensions (such as the club house), only the rooms should see the call information display.
- For external calls from the public switched telephone network (PSTN) to the front desk or guest rooms, the call information of the caller should not display if the display settings are restricted.
- For all calls to the front desk, the call information of internal calls should display.
- When the front desk transfers a call from a guest room to security, the room phone shows only the dialed number for the front desk.

Enabling Call Display Restrictions

The basis for the functionality of the Call Display Restrictions feature is calls being routed through different translation patterns before the calls are extended to the actual device. Users then dial the appropriate translation pattern numbers to achieve the display restrictions.

Translation Pattern Configuration

To enable Call Display Restrictions, configure translation patterns with different levels of display restrictions by choosing the appropriate option for the calling line ID presentation and the connected line ID presentation parameters.

See the “Configuring the Translation Pattern Parameters” section on page 4-7 for additional information about these parameters.

Tip

You must configure partitions and calling search spaces, along with translation patterns. For more information about these configurations, see the Translation Pattern Configuration chapter in the Cisco Unified Communications Manager Administration Guide.
Phone Configuration/User Device Profile Configuration

Next, enable the “Ignore Presentation Indicators (internal calls only)” parameter to ignore any presentation restriction that is received for internal calls and to ensure that the device will display the call information of the remote party.

See the “Configuring the Phone Configuration” section on page 4-8 for more information about this setting.

(For users who log in to phones that are enabled for Extension Mobility, configure this setting from the Cisco Unified Communications Manager Administration Device Profile Configuration window as well. For more information about interactions with Extension Mobility, see the “Extension Mobility” section on page 4-6.)

Connected Number Display

When a call routes through a translation or route pattern, routes to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application, the connected number display updates to show the modified number or redirected number.

To turn off phone display updates, so the phone displays only the dialed digits, set the Cisco CallManager service parameter “Always Display Original Dialed Number” to true. When this service parameter specifies true, the originating phone displays only the dialed digits for the duration of the call.

System Requirements for Call Display Restrictions

The following software components support Call Display Restrictions:
- Cisco Unified Communications Manager

The following devices support Call Display Restrictions:
- Cisco Unified IP Phone 6900 Series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 Series
- Cisco Unified IP Phone 8900 Series
- Cisco Unified IP Phone 9900 Series
- H.323 clients
- CTI ports
- Cisco IP Communicator

Scenarios for Using Call Display Restrictions

The following scenarios provide examples for using Call Display Restrictions:
- Front Desk calls Room-1—Both phones display the call information of each other.
- Front Desk calls Room-1, and Front Desk transfers the call to Room-2—The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
- External (PSTN) calls the Front Desk—The Front Desk honors the display settings of the external caller.
- External (PSTN) calls Room-1—Room-1 honors the presentation of the external caller; the external caller cannot see the call information display of Room-1.
• Room-1 calls Front Desk—Both phones display the call information of each other.
• Room-1 calls Room-2—Neither phone can see the call information display of the other.
• Room-1 calls Front Desk, and Front Desk transfers the call to Room-2—The final connected parties, Room-1 and Room-2, cannot see the call information display of each other.
• Room-1 calls Front Desk-1, and Front Desk-1 transfers the call to Front Desk-2—The final connected parties, Room-1 and Front Desk-2, can see the call information display of each other.
• Room-1 calls Room-2, and Room-2 transfers the call to Front Desk—Room-1 and Front Desk see the call information display of each other.
• Club House calls Room-1—Club House cannot display the call information; Room-1 can see the call information display.
• All parties in a conference call—All phones see “To Conference” for the call information display.
• Room-1 calls Club House, and Club House manager has all calls forwarded to his mobile—Room-1 sees the Club House number only.

Interactions

The following sections describe how the Call Display Restrictions feature interacts with Cisco Unified Communications Manager applications and call processing:

• Call Park, page 4-5
• Conference List, page 4-6
• Conference and Voice Mail, page 4-6
• Extension Mobility, page 4-6

The connected number display restriction applies to all calls that originate in the cluster. When set to true, this setting interacts transparently with existing Cisco Unified Communications Manager applications, features, and call processing. The setting applies to all calls that terminate inside or outside the cluster.

Call Park

When the Call Display Restrictions feature is used with Call Park, you must configure an associated translation pattern for each individual call park number to preserve the Call Display Restrictions feature; you cannot configure a single translation pattern to cover a range of call park numbers.

Consider the following scenario as an example:

1. The system administrator creates a call park range of 77x and places it in a partition called P_ParkRange. (The phones in the guest rooms can see the P_ParkRange partition is made visible to the phones in the guest rooms by inclusion of it in the calling search space of the phones (CSS_FromRoom).)
2. The administrator configures a separate translation pattern for each call park directory number and configures the display settings to Restricted. (In the current scenario, the administrator creates translations patterns for 770, 771, 772...779.)
Configuring Call Display Restrictions

For the Call Display Restrictions feature to work correctly, the administrator must configure separate translation patterns and not a single translation pattern for a range of numbers (such as 77x or 77[0-9]).

3. Room-1 calls Room-2.
4. Room-2 answers the call, and Room-1 parks the call.
5. When Room-1 retrieves the call, Room-2 does not see Room-1 call information display.

See the “Call Park and Directed Call Park” section on page 5-1 for additional information about using the Call Park feature.

Conference List

When you use Call Display Restrictions, you restrict the display information for the list of participants in a conference. For more information about conference lists, see the “Phone Features” section in the Cisco Unified IP Phones chapter in the Cisco Unified Communications Manager System Guide.

Conference and Voice Mail

When Call Display Restrictions are used with features such as conference and voice mail, the call information display on the phones reflects that status. For example, when the conference feature is invoked, the call information display shows “To Conference.” When voice mail is accessed by choosing the “Messages” button, the call information display shows “To Voicemail.”

Extension Mobility

To use Call Display Restrictions with Extension Mobility, enable the “Ignore Presentation Indicators (internal calls only)” parameter in both the Cisco Unified Communications Manager Administration Phone Configuration window and the Cisco Unified Communications Manager Administration Device Profile Configuration window.

When you enable Call Display Restrictions with Extension Mobility, the presentation or restriction of the call information depends on the line profile that is associated with the user who is logged in to the device. That is, the configuration that is entered in the user device profile (associated with the user) overrides the configuration that is entered in the phone configuration (of the phone that is enabled for Extension Mobility).

Configuring Call Display Restrictions

To use Call Display Restrictions, make sure that you perform the following Cisco Unified Communications Manager configurations:

- Configure partitions and calling search spaces before you add a translation pattern.
- Configure translation patterns with different levels of display restrictions.
- From the Phone Configuration window, check the “Ignore Presentation Restriction (internal calls only)” check box to ensure that the call information display for internal calls is always visible.
• Configure individual, associated translation patterns for each individual Call Park directory number, to work with the Call Park feature.

• Set the “Always Display Original Dial Number” service parameter to True to ensure privacy and to block connected number updates for redirected calls.

This section contains the following topics:

• Configuration Checklist for Call Display Restrictions, page 4-1
• Configuring the Translation Pattern Parameters, page 4-7
• Configuring the Phone Configuration, page 4-8
• Sample Configurations, page 4-9

Tip
Before you configure call display restrictions, review the “Configuration Checklist for Call Display Restrictions” section on page 4-1.

## Configuring the Translation Pattern Parameters

Configure the following parameters from the Cisco Unified Communications Manager Administration Translation Pattern Configuration window.

Tip
For outgoing calls, the translation pattern setting at the terminating end can override the originating Cisco Unified Communications Manager cluster settings.

### Calling Line ID Presentation

Cisco Unified Communications Manager uses calling line ID presentation as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose one of the following options to allow or restrict the display of the calling party phone number on the called party phone display for this translation pattern:

• Default—This option does not change the calling line ID presentation.
• Allowed—Cisco Unified Communications Manager allows the display of the calling number.
• Restricted—Cisco Unified Communications Manager blocks the display of the calling number.

Note
If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the system modifies the calling line presentation with the translation or route pattern setting.

### Connected Line ID Presentation

Cisco Unified Communications Manager uses connected line ID presentation as a supplementary service to allow or restrict the called party phone number on a per-call basis. Choose one of the following options to allow or restrict the display of the connected party phone number on the calling party phone display for this translation pattern:

• Default—This option does not change the connected line ID presentation.
• Allowed—This option displays the connected party phone number.
Configuring Call Display Restrictions

- **Restricted**—Cisco Unified Communications Manager blocks the display of the connected party phone number.

**Note**

If the incoming call goes through a translation or route pattern and the connected line ID presentation field is set to allowed or restricted, the system modifies the connected line presentation indicator with the translation or route pattern setting.

**Note**

If the connected number display restriction is enabled, the connected number display does not update for modified numbers or redirected calls.

**Examples**

- For calls that are made from one guest room to another, configure the calling line ID presentation and the connected line ID presentation to restricted to ensure that the call information does not display.
- For calls that are made from the front desk to a guest room, configure the calling line ID presentation to allowed and the connected line ID presentation to restricted to ensure both parties can see the call information.

**Tip**

For more information about calling party transformations and connected party transformations, see the *Understanding Route Plans* chapter in the *Cisco Unified Communications Manager System Guide*.

Configuring the Phone Configuration

To complete the configuration of the Call Display Restrictions feature, check the “Ignore Presentation Indicators (internal calls only)” check box from the Cisco Unified Communications Manager Administration Phone Configuration window.

For use with Extension Mobility, also configure this setting from the Cisco Unified Communications Manager Administration Device Profile Configuration window.

When you set the “Ignore Presentation Indicators (internal calls only)” field,

- Cisco Unified Communications Manager always displays the remote party call information if the other party is internal.
- Cisco Unified Communications Manager does not display the remote party call information if the other party is external and the display presentation is restricted.

**Note**

Ensure the calling line ID presentation and the connected line ID presentation are configured with the “Ignore Presentation Indicators (internal calls only)” parameter for Cisco Unified Communications Manager to ignore the presentation settings of internal callers. For incoming external calls, the system maintains the received presentation indicators even if the “Ignore Presentation Indicators (internal calls only)” parameter is set.

- For phones that are used at the hotel front desk, check the “Ignore Presentation Indicators (internal calls only)” check box, so the front desk can always see the call information display for internal calls.
Sample Configurations

The following information provides sample configurations to enable the Call Display Restrictions feature and includes the following topics:

- Partitions, page 4-9
- Calling Search Spaces, page 4-10
- Devices and Gateways, page 4-10
- Translation Patterns, page 4-11
- Call Park, page 4-13

Partitions

From the Cisco Unified Communications Manager Administration Partition Configuration window, configure the following partitions:

- Insert a real partition P_Room
- Insert a real partition P_FrontDesk
- Insert a real partition P_Club
- Insert a real partition P_PSTN
- Insert a translation partition P_CallsFromRoomToRoom
- Insert a translation partition P_CallsFromRoomToFrontDesk
- Insert a translation partition P_CallsFromRoomToClub
- Insert a translation partition P_CallsFromRoomToPSTN
- Insert a translation partition P_CallsFromFrontDeskToRoom
- Insert a translation partition P_CallsFromFrontDeskToFrontDesk
- Insert a translation partition P_CallsFromFrontDeskToClub
- Insert a translation partition P_CallsFromFrontDeskToPSTN
- Insert a translation partition P_CallsFromPSTN
- Insert a translation partition P_CallsFromClubToRoom
- Insert a translation partition P_CallsFromClubToFrontDesk
- Insert a translation partition P_FrontDeskToParkNumber
- Insert a translation partition P_RoomToParkNumber
- Insert a translation partition P_ParkNumberRange
Chapter 4  Call Display Restrictions

Configuring Call Display Restrictions

Calling Search Spaces

From the Cisco Unified Communications Manager Administration Calling Search Space Configuration window, configure the following calling search spaces:

- Insert a calling search space CSS_Room {P_Room}
- Insert a calling search space CSS_FrontDesk {P_FrontDesk}
- Insert a calling search space CSS_Club {P_Club}
- Insert a calling search space CSS_PSTN {P_PSTN}
- Insert a calling search space CSS_FromRoom
  { P_CallsFromRoomToFrontDesk, P_CallsFromRoomToRoom, P_CallsFromRoomToClub, 
P_CallsFromRoomToPSTN, P_RoomToParkNumber, P_ParkNumberRange}
- Insert a calling search space CSS_FromFrontDesk
  { P_CallsFromFrontDeskToRoom, P_CallsFromFrontDeskToClub, 
P_CallsFromFrontDeskToPSTN, P_CallsFromFrontDeskToFrontDesk}
- Insert a calling search space CSS_FromPSTN
  { P_CallsFromPSTN}
- Insert a calling search space CSS_FromClub
  { P_CallsFromClubToRoom, P_CallsFromClubToFrontDesk}
- Insert a calling search space CSS_RoomParkRange
  {P_ParkNumberRange}

Devices and Gateways

From the Cisco Unified Communications Manager Administration Phone Configuration window and from the Cisco Unified Communications Manager Administration Gateway Configuration window, configure the following phones and configure the following gateway:

- Configure phone A (Room-1) with partition P_Room and device/line calling search space CSS_FromRoom
  { P_Phones, CSS_FromRoom} : 221/Room-1
- Configure phone B (Room-2) with partition P_Room and device/line calling search space CSS_FromRoom
  { P_Phones, CSS_FromRoom} : 222/Room-2
- Configure phone C (Front Desk-1) with partition P_FrontDesk and device/line calling search space CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled
  { P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 100/Reception
- Configure phone D (Front Desk-2) with partition P_FrontDesk and device/line calling search space CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled
  { P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 200/Reception
- Configure phone E (Club) with partition P_Club and calling search space CSS_FromClub
  { P_Club, CSS_FromClub} : 300/Club
- Configure PSTN Gateway E with route pattern P_PSTN and calling search space CSS_FromPSTN
  {CSS_FromPSTN}, RoutePattern {P_PSTN}
Translation Patterns

From the Cisco Unified Communications Manager Administration Translation Pattern Configuration window, configure the following translation patterns:

- Insert a translation pattern TP1 as 1XX
  Partition: P_CallsFromRoomToFrontDesk
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  \{P_CallsFromRoomToFrontDesk, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed\}

- Insert a translation pattern TP2 as 2XX
  Partition: P_CallsFromRoomToRoom
  CSS: CSS_Room
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Restricted
  \{P_CallsFromRoomToRoom, CSS_Room, Calling Line/Name - Restricted, Connected Line/Name - Restricted\}

- Insert a translation pattern TP3 as 3XX
  Partition: P_CallsFromRoomToClub
  CSS: CSS_Club
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  \{P_CallsFromRoomToClub, CSS_Club, Calling Line/Name - Restricted, Connected Line/Name - Allowed\}

- Insert a translation pattern TP4 as 9XXXX with called party transform mask as XXX
  Partition: P_CallsFromRoomToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Default
  \{P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default\}

- Insert a route pattern RP5 as 9.XXXXX X with discard digits as predot (DDI : PreDot)
  Partition: P_CallsFromRoomToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Default
  \{P_CallsFromRoomToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default\}

- Insert a translation pattern TP6 as 2XX
  Partition: P_CallsFromFrontDeskToRoom
  CSS: CSS_Room
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Restricted
  \{P_CallsFromFrontDeskToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted\}

- Insert a translation pattern TP7 as 1XX
  Partition: P_CallsFromFrontDeskToFrontDesk
  CSS: CSS_FrontDesk
Configuring Call Display Restrictions

Calling Line ID Presentation and Calling Name Presentation: Allowed
Connected Line ID Presentation and Connected Name Presentation: Allowed
{P_CallsFromFrontDeskToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}

- Insert a translation pattern TP8 as 3XX
  Partition: P_CallsFromFrontDeskToClub
  CSS: CSS_Club
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  {P_CallsFromFrontDeskToClub, CSS_Club, Calling Line/Name - Allowed, Connected Line/Name - Allowed}

- Insert a translation pattern TP9 as 9XXXX
  Partition: P_CallsFromFrontDeskToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Default
  {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Allowed, Connected Line/Name - Default}

- Insert a route pattern RP10 as 9.XXXX with discard digits as predot
  Partition: P_CallsFromFrontDeskToPSTN
  CSS: CSS_PSTN
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Default
  {P_CallsFromFrontDeskToPSTN, CSS_PSTN, Calling Line/Name - Restricted, Connected Line/Name - Default}

- Insert a translation pattern TP11 as 1XX
  Partition: P_CallsFromClubToFrontDesk
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  {P_CallsFromClubToFrontDesk, CSS_FrontDesk, Calling Line/Name - Allowed, Connected Line/Name - Allowed}

- Insert a translation pattern TP12 as 2XX
  Partition: P_CallsFromClubToRoom
  CSS: CSS_Room
  Calling Line ID Presentation and Calling Name Presentation: Allowed
  Connected Line ID Presentation and Connected Name Presentation: Restricted
  {P_CallsFromClubToRoom, CSS_Room, Calling Line/Name - Allowed, Connected Line/Name - Restricted}

- Insert a translation pattern TP13 as 1XX
  Partition: P_CallsFromPSTN
  CSS: CSS_FrontDesk
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Allowed
  {P_CallsFromPSTN, CSS_FrontDesk, Calling Line/Name - Restricted, Connected Line/Name - Allowed}
Call Park

From the Cisco Unified Communications Manager Administration Call Park Number Configuration window, configure the following items for the Call Park feature:

- Insert a Call Park directory number 888X
  Call Park Number Range: P_ParkNumberRange/888X

- Configure the translation patterns for the call park retrieval from room: TP (11-20): 8880 to 8889
  Partition: P_RoomToParkNumber
  CSS: CSS_RoomParkRange
  Calling Line ID Presentation and Calling Name Presentation: Restricted
  Connected Line ID Presentation and Connected Name Presentation: Restricted

Sample Call Flow

Figure 4-1 shows a graphic representation of a sample call flow, with a description of how the Call Display Restrictions feature works in this scenario.

1. Room-1 calls Room-2 (directory number 222).
2. Room-1 has CSS_FromRoom, so Room-1 can access only phones that are in the P_CallsFromRoomToRoom partition.
3. The P_CallsFromRoomToRoom partition contains 2XX, but it does not contain directory number 222 (Room-2).
4. The call routes to translation pattern TP:2XX, which is configured to restrict display information.
5. The TP:2XX translation pattern can access the P_Room partition because it is configured with the CSS_Room calling search space.
6. The CSS_Room calling search space contains directory number 222 (Room-2).
7. The call connects to Room-2, but the TP:2XX translation pattern restricts the display information.
Setting the Service Parameter for Connected Number Display Restriction

The connected number display restriction restricts the connected line ID presentation to dialed digits only. This option addresses customer privacy issues as well as connected number displays that are meaningless to phone users.

As administrator, you configure the connected number display restriction parameter by accessing System > Service Parameters in Cisco Unified Communications Manager Administration—choose the server where the Cisco CallManager service runs and then choose the Cisco CallManager service.

Set the Always Display Original Dialed Number service parameter to True to enable this feature. The default setting specifies false.

Related Topics

- Configuration Checklist for Call Display Restrictions, page 4-1
- Introducing Call Display Restrictions, page 4-2
- System Requirements for Call Display Restrictions, page 4-4
- Scenarios for Using Call Display Restrictions, page 4-4
- Interactions, page 4-5
- Configuring Call Display Restrictions, page 4-6
- Setting the Service Parameter for Connected Number Display Restriction, page 4-14
- Translation Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide
- Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Partition Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phones, Cisco Unified Communications Manager System Guide
- Phone Features, Cisco Unified Communications Manager System Guide

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone user documentation and release notes (all models)
This chapter describes the Call Park feature, which is a hold function, and the Directed Call Park feature, which is a transfer function. Cisco recommends that you treat these two features as mutually exclusive: enable one or the other, but not both. If you do enable both, ensure that the numbers that are assigned to each are exclusive and do not overlap.

This chapter provides the following information about call park (including park monitoring for Cisco Unified IP Phones 8961, 9951, and 9971), and directed call park (including assisted directed call park):

**Call Park**
- Call Park Configuration Checklist, page 5-2
- Introducing Call Park, page 5-4
- System Requirements for Call Park, page 5-7
- Interactions and Restrictions, page 5-8
- Installing and Activating Call Park, page 5-10
- Configuring Call Park, page 5-11
- Setting the Service Parameters for Call Park, page 5-11
- Finding a Call Park Number, page 5-11
- Configuring a Call Park Number, page 5-13
- Call Park Configuration Settings, page 5-13
- Deleting a Call Park Number, page 5-15
- Related Topics, page 5-30

**Park Monitoring (Cisco Unified IP Phones 8961, 9951, and 9971 only)**
- Park Monitoring for Cisco Unified IP Phones 8961, 9951, and 9971, page 5-16

**Directed Call Park**
- Directed Call Park Configuration Checklist, page 5-3
- Introducing Directed Call Park, page 5-19
- System Requirements for Directed Call Park, page 5-20
- Interactions and Restrictions, page 5-20
- Installing and Activating Directed Call Park, page 5-23
- Setting the Service Parameters for Directed Call Park, page 5-23
Call Park Configuration Checklist

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. You can park only one call at each call park extension number.

Table 5-1 provides a checklist to configure Call Park. For more information on the Call Park feature, see the “Introducing Call Park” section on page 5-4 and the “Related Topics” section on page 5-30.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure a partition for call park extension numbers to make partition available only to users who have the partition in their calling search space.</td>
</tr>
<tr>
<td></td>
<td>Related procedures and topics</td>
</tr>
<tr>
<td></td>
<td>Partition Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Media Termination Point Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure a unique call park number or define a range of call park extension numbers for each Cisco Unified Communications Manager in the cluster.</td>
</tr>
<tr>
<td></td>
<td>Configuring a Call Park Number, page 5-13</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Add all servers that call park uses to the appropriate Cisco Unified Communications Manager group. Note: Servers and Cisco Unified Communications Managers get configured during installation.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager Group Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
Directed Call Park Configuration Checklist

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number. See the “System Requirements for Directed Call Park” section on page 5-20 for a list of the phone models that support the BLF.

Cisco Unified Communications Manager can park only one call at each directed call park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the directed call park number at which the call is parked. Configure the retrieval prefix in the Directed Call Park Configuration window.

Table 5-2 provides a checklist to configure directed call park. For more information, see the “Introducing Directed Call Park” section on page 5-19 and the “Related Topics” section on page 5-30.
**Introducing Call Park**

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. You can park only one call at each call park extension number.

---

**Table 5-2 Directed Call Park Configuration Checklist**

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure a partition for directed call park numbers to make the partition available only to users who have the partition in their calling search space. To successfully retrieve a parked call, the calling search space from which the user is retrieving the call must contain the partition that includes the directed call park number.</td>
</tr>
<tr>
<td></td>
<td>Related procedures and topics</td>
</tr>
<tr>
<td></td>
<td><strong>Partition Configuration Settings</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td><strong>Media Termination Point Configuration</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td><strong>Calling Search Space Configuration</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure a unique directed call park number or define a range of directed call park numbers. You must specify a range by using wildcards. For example, the range 40XX configures the range as 4000 to 4099.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> Do not enter a range by using dashes (such as 4000-4040).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can monitor only individual directed call park numbers with the directed call park BLF. If you configure a range of numbers, the BLF cannot support monitoring of the busy/idle status of the range or of any number within the range.</td>
</tr>
<tr>
<td></td>
<td><strong>Configuring a Directed Call Park Number</strong>, page 5-24</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign the Standard User softkey template to each device that has directed call park access.</td>
</tr>
<tr>
<td></td>
<td><strong>Softkey Template Configuration</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>For phone models that support the directed call park BLF, configure the phone button template to include one or more Call Park BLF buttons and configure the directed call park BLF settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Guidelines for Customizing Phone Button Templates</strong>, <em>Cisco Unified Communications Manager System Guide</em></td>
</tr>
<tr>
<td></td>
<td><strong>Configuring BLF/Directed Call Park Buttons</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Notify users that the directed call park feature is available.</td>
</tr>
<tr>
<td></td>
<td>See the phone documentation for instructions on how users access directed call park features on their Cisco Unified IP Phone.</td>
</tr>
</tbody>
</table>
The Call Park feature works within a Cisco Unified Communications Manager cluster, and each Cisco Unified Communications Manager in a cluster must have call park extension numbers defined. (For information about using call park across clusters, see the “Using Call Park Across Clusters” section on page 5-6.) You can define either a single directory number or a range of directory numbers for use as call park extension numbers. Ensure that the directory number or range of numbers is unique.

Valid call park extension numbers comprise integers and the wildcard character, X. You can configure a maximum of XX in a call park extension number (for example, 80XX), which provides up to 100 call park extension numbers. When a call gets parked, Cisco Unified Communications Manager chooses the next call park extension number that is available and displays that number on the phone.

Cisco Unified Communications Manager can park only one call at each call park extension number.

If users will use call park across servers in a cluster, ensure each Cisco Unified Communications Manager server in a cluster has call park extension numbers that are configured. See the “Configuring a Call Park Number” section on page 5-13 for configuration details.

Using the Call Park Feature

Figure 5-1 illustrates the call park process.

1. User on phone A calls phone B.
2. User on phone A wants to take the call in a conference room for privacy. Phone A user presses the Park softkey or button.
3. The Cisco Unified Communications Manager server to which phone A is registered sends the first available call park directory, 1234, which displays on phone A. The user on phone A watches the display for the call park directory number (so he can dial that directory number on phone C).
4. The user on phone A leaves the office and walks to an available conference room where the phone is designated as phone C. The user goes off-hook on phone C and dials 1234 to retrieve the parked call.
5. The system establishes call between phones C and B.

Figure 5-1: Call Park Process
Using Call Park Across Clusters

Users can dial the assigned route pattern (for example, a route pattern for an intercluster trunk could be 80XX) and the call park number (for example 8022) to retrieve parked calls from another Cisco Unified Communications Manager cluster. Additionally, you must ensure that calling search spaces and partitions are properly configured.

See the following example.

Example of Retrieving Parked Calls from Another Cluster


Cluster A includes call park numbers in the range of 81xx. Cluster B includes call park numbers in the range of 82xx, which the administrator configured.

Cluster A includes route patterns that are configured to other cluster park ranges as 82xx (routes to Cluster B). Cluster B includes route patterns that are configured to other cluster park ranges as 81xx (routes to Cluster A).

When user A1 parks a call at 8101, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. When user B1 parks a call at 8202, all users (which have correct partitions configured) in Cluster A and Cluster B can retrieve the parked call because of the route pattern configuration. See Figure 5-2.
System Requirements for Call Park

To operate, call park requires the following software component:

- Cisco Unified Communications Manager

The following IP phones (SCCP and SIP) support call park with the Park softkey in the Standard User and Standard Feature softkey templates:

- Cisco Unified IP Phones 6900 (except 6901 and 6911)
- Cisco Unified IP Phones 7900 (except 7921, 7925, 7935, 7936, 7937)

Additional Information

See the “Related Topics” section on page 5-30.
Interactions and Restrictions

The following sections describe the interactions and restrictions for call park:

- Interactions, page 5-8
- Restrictions, page 5-10

CTI Applications

CTI applications access call park functionality, including monitoring activity on call park DNs. To monitor a call park DN, you must add an application or end user that is associated with the CTI application to the Standard CTI Allow Call Park Monitoring user group.
Music On Hold

Music on hold allows users to place calls on hold with music that a streaming source provides. Music on hold allows two types of hold:

- User hold—The system invokes this type of hold when a user presses the Hold button or Hold softkey.
- Network hold—This type of hold takes place when a user activates the transfer, conference, or call park feature, and the hold automatically gets invoked.

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to call park. See the Route Plan Report chapter in the Cisco Unified Communications Manager Administration Guide.

Calling Search Space and Partitions

Assign the Call Park directory number or range to a partition to limit call park access to users on the basis of the device calling search space. See Calling Search Space Configuration and Partition Configuration in the Cisco Unified Communications Manager Administration Guide.

Immediate Divert

Call park supports Immediate Divert (iDivert or Divert softkey). For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to a voice-messaging mailbox by pressing the iDivert or Divert softkey. User A receives the voice-messaging mailbox greeting of user B.

Barge

The following paragraphs describe the differences between Barge and cBarge with call park.

Barge with Call Park

The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggy backs” on the target phone. The target phone includes most of the common features, even when the target is being barged; therefore, the barge initiator has no feature access. When the target parks a call, the barge initiator then must release its call (the barge).

cBarge with Call Park

The target and barge initiator act as peers. The cBarge feature uses a conference bridge, which makes it behave similar to a MeetMe conference. Both phones (target and barge initiator) have full access to their features.

Directed Call Park

Cisco recommends that you do not configure both directed call park and the Park softkey for call park, but the possibility exists to configure both. If you configure both, ensure that the call park and directed call park numbers do not overlap.
QSIG Intercluster Trunks

When a user parks a call across a QSIG intercluster trunk or a QSIG gateway trunk, the caller who has been parked (the parkee) does not see the To parked number message. The phone continues to display the original connected number. The call has been parked, and the user who parked the call can retrieve it. When the call is retrieved from the parked state, the call continues, but the caller who was parked does not see the newly connected number.

Additional Information
See the “Related Topics” section on page 5-30.

Restrictions

The following restrictions apply to call park:

• Cisco Unified Communications Manager can park only one call at each call park extension number.
• Ensure each call park directory number, partition, and range is unique within the Cisco Unified Communications Manager cluster.
• For shared line devices across nodes, the line will register to the node on which the device registers first. For example, if a device from subscriber2 registers first and the line is created in subscriber2 and the publisher server, the line belongs to subscriber2. Each node must be configured with the call park number.
• To achieve failover/fallback, configure call park numbers on the publisher server and subscriber nodes. With this configuration, when the primary node is down, the line/device association gets changed to the secondary node, and the secondary node call park number gets used.
• Each Cisco Unified Communications Manager to which devices are registered needs its own unique call park directory number and range.
• Cisco Unified Communications Manager Administration does not validate the call park numbers or range that you use to configure call park. To help identify invalid numbers or ranges and potential range overlaps, use the Cisco Unified Communications Manager Dialed Number Analyzer tool.
• If any call park numbers are configured for Cisco Unified Communications Manager on a node that is being deleted in the Server Configuration window (System > Server), the server deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
• Cisco Unified Communications Manager Administration does not check that the value that is entered for Call Park Reversion Timer is less than the value that is entered for the Call Park Display Timer. If you entered a Call Park Reversion Timer value that is less than the Call Park Display Timer, call park numbers will not display on the phone.

See the “Configuring a Call Park Number” section on page 5-13 for configuration details.

Additional Information
See the “Related Topics” section on page 5-30.

Installing and Activating Call Park

Call park, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.
Configuring Call Park

This section contains the following information:

- Setting the Service Parameters for Call Park, page 5-11
- Finding a Call Park Number, page 5-11
- Configuring a Call Park Number, page 5-13
- Deleting a Call Park Number, page 5-15

Tip

Before you configure call park, review the “Call Park Configuration Checklist” section on page 5-2.

Setting the Service Parameters for Call Park

Cisco Unified Communications Manager provides two clusterwide service parameters for call park: Call Park Display Timer and Call Park Reversion Timer. Each service parameter includes a default and requires no special configuration.

- Call Park Display Timer—Default specifies 10 seconds. This parameter determines how long a call park number displays on the phone that parked the call. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured.

- Call Park Reversion Timer—Default specifies 60 seconds. This parameter determines the time that a call remains parked. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. When this timer expires, the parked call returns to the device that parked the call. If a hunt group member parks a call that comes through a hunt pilot, the call goes back to the hunt pilot upon expiration of the Call Park Reversion Timer.

Note

To set the timers, choose System > Service Parameters and update the Call Park Display Timer and the Call Park Reversion Timer fields in the Clusterwide Parameters (Feature-General) pane.

Additional Information

See the “Related Topics” section on page 5-30.

Finding a Call Park Number

Because you may have several call park numbers in your network, Cisco Unified Communications Manager lets you locate specific call park numbers on the basis of specific criteria. Use the following procedure to locate call park numbers.
During your work in a browser session, Cisco Unified Communications Manager Administration retains your call park number search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your call park number search preferences until you modify your search or close the browser.

**Procedure**

**Step 1**
Choose **Call Routing > Call Park**.

The Find and List Call Park Numbers window displays.

**Step 2**
To find all records in the database, ensure the dialog box is empty; go to **Step 3**.

To filter or search records:
- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

**Note**
To add additional search criteria click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the **Clear Filter** button to remove all added search criteria.

**Step 3**
Click **Find**.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Note**
You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

**Step 4**
From the list of records that display, click the link for the record that you want to view.

**Note**
To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

**Additional Information**

See the “Related Topics” section on page 5-30.
Configuring a Call Park Number

This section describes how to add, copy, and update a single call park extension number or range of extension numbers.

Procedure

**Step 1** Choose **Call Routing > Call Park**.

**Step 2** Perform one of the following tasks:

- To add a new Call Park Number, click **Add New**.
- To copy a Call Park Number, use the procedure in the “Finding a Call Park Number” section on page 5-11 to locate the call park number or range of numbers. Click the Copy icon.
- To update a Call Park Number, use the procedure in the “Finding a Call Park Number” section on page 5-11 to locate the call park number or range of numbers.

The Call Park Number Configuration window displays.

**Step 3** Enter or update the appropriate settings as described in Table 5-3.

**Step 4** To save the new or changed call park numbers in the database, click **Save**.

**Additional Information**

See the “Related Topics” section on page 5-30.

Call Park Configuration Settings

The Call Park feature allows you to place a call on hold, so it can be retrieved from another phone in the Cisco Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as call park extension numbers. You can park only one call at each call park extension number. Table 5-1 provides the configuration checklist for Call Park.
Table 5-3 describes the call park configuration settings. For related procedures, see the “Related Topics” section on page 5-30.

### Table 5-3  Call Park Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call Park Number/Range | Enter the call park extension number. You can enter literal digits or the wildcard character X (the system allows one or two Xs). For example, enter 5555 to define a single call park extension number of 5555 or enter 55XX to define a range of call park extension numbers from 5500 to 5599.  
  **Note** You can create a maximum of 100 call park numbers with one call park range definition. Make sure that the call park numbers are unique.  
  **Note** You cannot overlap call park numbers between Cisco Unified Communications Manager servers. Ensure that each Cisco Unified Communications Manager server has its own number range.  
  **Note** The call park range is selected from the list of servers where the call originates. For example, if phone A (registered to node A) calls phone B (registered to node B) and the phone B user presses Park, phone B requires a call park range in the CSS that resides on node A. In a multinode environment where phones and gateways communicate with various nodes and where calls that originate from any server may need to be parked, the phones require a CSS that contains call park ranges from all servers. |
| Description            | Provide a brief description of this call park number. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>) |
| Partition              | If you want to use a partition to restrict access to the call park numbers, choose the desired partition from the drop-down list box. If you do not want to restrict access to the call park numbers, choose <None> for the partition.  
  See **Searching for a Partition** in the *Cisco Unified Communications Manager Administration Guide* for instructions on finding a partition when there are a large number of them configured.  
  **Note** Make sure that the combination of call park extension number and partition is unique within the Cisco Unified Communications Manager cluster. |
Chapter 5  Call Park and Directed Call Park

Configuring Call Park

Deleting a Call Park Number

This section describes how to delete call park numbers from the Cisco Unified Communications Manager database.

Procedure

- **Step 1** Using the procedure in the “Finding a Call Park Number” section on page 5-11, locate the call park number or range of numbers.
- **Step 2** Click the call park number or range of numbers that you want to delete.
- **Step 3** Click **Delete**.

**Note** You can delete multiple call park numbers from the Find and List Call Park Numbers window by checking the check boxes next to the appropriate call park numbers and clicking **Delete Selected**. You can delete all call park numbers in the window by clicking **Select All** and then clicking **Delete Selected**.

### Table 5-3  Call Park Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Using the drop-down list box, choose the Cisco Unified Communications Manager to which these call park numbers apply. <strong>Note</strong> You can create a maximum of 100 call park numbers with one call park range definition. Make sure that the call park numbers are unique. <strong>Note</strong> You cannot overlap call park numbers between Cisco Unified Communications Manager servers. Ensure that each Cisco Unified Communications Manager server has its own number range. <strong>Note</strong> The call park range is selected from the list of servers where the call originates. For example, if Phone A (registered to node A) calls Phone B (registered to Node B) and the phone B user presses Park, Phone B requires a call park range in the CSS that resides on Node A. In a multinode environment comprised of phones and gateways talking to various nodes, where calls originating from any server may need to be parked, the phones require a CSS that contains call park ranges from all servers.</td>
</tr>
</tbody>
</table>
Park Monitoring for Cisco Unified IP Phones 8961, 9951, and 9971

Park monitoring is supported only when a Cisco Unified IP Phone 8961, 9951, or 9971 (SIP) parks a call. Park monitoring then monitors the status of a parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved using the same call bubble on the parker’s phone.

**Note**
Configuring call park numbers and settings are the same procedures as for other phone models.

The following sections describe the options for configuring park monitoring:

- Setting the Service Parameters for Park Monitoring, page 5-16
- Setting Park Monitoring Parameters in Directory Number Configuration Window, page 5-18
- Setting Park Monitoring Parameter in Hunt Pilot Configuration Window, page 5-18

**Setting the Service Parameters for Park Monitoring**

Cisco Unified Communications Manager provides three clusterwide service timer parameters for park monitoring: Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer. Each service parameter includes a default and requires no special configuration. These timer parameters apply to park monitoring only; the Call Park Display Timer and Call Park Reversion Timer are not used for park monitoring.
See **Table 5-4** for descriptions of these parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring Reversion Timer</td>
<td>Default value specifies 60 seconds. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires. You can override the value that this service parameter specifies on a per-line basis in the Directory Number Configuration window (<strong>Call Routing &gt; Directory Number</strong>), in the Park Monitoring section. Specify a value of 0 to immediately utilize the periodic reversion interval that the Park Monitoring Periodic Reversion Timer service parameter specifies. For example, if this parameter is set to zero and the Park Monitoring Periodic Reversion Timer is set to 15, the user is prompted about the parked call immediately and every 15 seconds thereafter until the Park Monitoring Forward No Retrieve Timer expires.</td>
</tr>
<tr>
<td>Park Monitoring Periodic Reversion Timer</td>
<td>Default value specifies 30 seconds. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. This parameter determines the interval (in seconds) that Cisco Unified Communications Manager waits before prompting the user again that a call has been parked. To connect to the parked call, the user can simply go off-hook during one of these prompts. Cisco Unified Communications Manager continues to prompt the user about the parked call as long as the call remains parked and until the Park Monitoring Forward No Retrieve Timer expires. Specify a value of 0 to disable periodic prompts about the parked call.</td>
</tr>
<tr>
<td>Park Monitoring Forward No Retrieve Timer</td>
<td>Default value specifies 300 seconds. Set this timer for each server in a cluster that has the Cisco CallManager service and call park configured. This parameter determines the number of seconds that park reminder notifications occur before the parked call forwards to the Park Monitoring Forward No Retrieve destination that is specified in the parker Directory Number Configuration window. (If no forward destination is provided in Cisco Unified Communications Manager Administration, the call returns to the line that parked the call.) This parameter starts when the Park Monitoring Reversion Timer expires. When the Park Monitoring Forward No Retrieve Timer expires, the call is removed from park and forwards to the specified destination or returned to the parker line.</td>
</tr>
</tbody>
</table>

**Note**

To set the timers, choose **System > Service Parameters** and update the Park Monitoring Reversion Timer, Park Monitoring Periodic Reversion Timer, and Park Monitoring Forward No Retrieve Timer fields in the **Clusterwide Parameters** (**Feature-General**) pane.

**Additional Information**

See the “Related Topics” section on page 5-30.
Setting Park Monitoring Parameters in Directory Number Configuration Window

The Directory Number Configuration window (Call Routing > Directory Number) contains an area called “Park Monitoring,” where you can configure the three parameters shown in Table 5-5.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Park Monitoring Forward No Retrieve</td>
<td>When the parkee is an external party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination External field. If the Forward No Retrieve Destination External field value is empty, the parkee gets redirected to the parker line.</td>
</tr>
<tr>
<td>Destination External</td>
<td></td>
</tr>
<tr>
<td>Park Monitoring Forward No Retrieve</td>
<td>When the parkee is an internal party, the call forwards to the specified destination in the parker Park Monitoring Forward No Retrieve Destination Internal field. If the Park Monitoring Forward No Retrieve Destination Internal field is empty, the parkee gets redirected to the parker line.</td>
</tr>
<tr>
<td>Destination Internal</td>
<td></td>
</tr>
<tr>
<td>Park Monitoring Reversion Timer</td>
<td>This parameter determines the number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires. Default: 60 seconds</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you configure a non-zero value, this value overrides the value of this parameter that is set in the Service Parameters window. However, if you configure a value of 0 here, the value in the Service Parameters window gets used.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 5-30.

Setting Park Monitoring Parameter in Hunt Pilot Configuration Window

When a call that was routed via the hunt list is parked, the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is used (unless it is blank) when the Park Monitoring Forward No Retrieve Timer expires. This value is configured in the Hunt Pilot Configuration window (Call Routing > Route/Hunt > Hunt Pilot). If the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter value is blank, then the call will be forwarded to the destination configured in the Directory Number Configuration window when the Park Monitoring Forward No Retrieve Timer expires.

Additional Information

See the “Related Topics” section on page 5-30.
Introducing Directed Call Park

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number. See Interactions and Restrictions, page 5-20, for a list of the phone models that support the BLF.

Cisco Unified Communications Manager can park only one call at each directed call park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the directed call park number at which the call is parked. Configure the retrieval prefix in the Directed Call Park Configuration window.

Example 1: Using the Directed Call Park Feature—Parked Call Gets Retrieved

The following example illustrates the use of the directed call park feature and retrieval of the parked call on Cisco Unified IP Phones (SCCP) only.

1. Users A1 and A2 connect in a call.
2. To park the call, A1 presses the Transfer softkey (or Transfer button, if available) and dials directed call park number 80 (for example) or presses the BLF button for directed call park number 80 (if the phone model supports the BLF button).
3. A1 either presses the Transfer softkey (or Transfer button) again or goes on hook to complete the directed call park transfer. This action parks A2 on directed call park number 80.

\[\text{Note}\]
The user can complete the transfer only by going on hook rather than pressing the Transfer softkey (or Transfer button) a second time if the Transfer On-hook Enabled service parameter is set to True. See “Onhook Call Transfer” in the Cisco Unified Communications Manager System Guide.

4. From any phone with a correctly configured partition and calling search space, user B1 dials the directed call park prefix (21, for example) followed by the directed call park number 80 to retrieve the call. B1 connects to A2.

Example 2: Using the Directed Call Park Feature—Parked Call Does Not Get Retrieved

The following example illustrates the use of the directed call park feature when the parked call does not get retrieved and reverts to the reversion number. This example illustrates how the feature works on Cisco Unified IP Phones (SCCP) only.

1. Users A1 and A2 connect in a call.
2. To park the call, A1 presses the Transfer softkey (or Transfer button, if available) and dials directed call park number 80 (for example) or presses the BLF button for directed call park number 80 (if the phone model supports the BLF button).
3. A1 either presses the Transfer softkey (or Transfer button) again or goes on hook to complete the directed call park transfer. This action parks A2 on directed call park number 80.

\[\text{Note}\]
The user can complete the transfer only by going on hook rather than pressing the Transfer softkey (or Transfer button) a second time if the Transfer On-hook Enabled service parameter is set to True. See “Onhook Call Transfer” in the Cisco Unified Communications Manager System Guide.
4. The call does not get retrieved before the Call Park Reversion Timer (service parameter) expires.
5. A2 reverts to the configured reversion number.

**Additional Information**
See the “Related Topics” section on page 5-30.

## System Requirements for Directed Call Park

To operate, Directed Call Park requires the following software component:
- Cisco Unified Communications Manager

A user can park and retrieve a call by using directed call park from any phone that can perform a transfer. Cisco VG248 Analog Phone Gateways also support directed call park.

The following IP phones (SCCP and SIP) support directed call park BLF:
- Cisco Unified IP Phone 6900 Series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 Series (except 7906, 7911, 7936, 7937)
- Cisco Unified Wireless IP Phone 7925
- Cisco Unified IP Phone Expansion Module (7914, 7915, 7916)
- Cisco Unified IP Color Key Expansion Module
- Cisco Unified IP Phone 8900 Series
- Cisco Unified IP Phone 9900 Series

The following phones that are running SCCP support directed call park BLF:
- Cisco Unified IP Phones (7940, 7960)

**Additional Information**
See the “Related Topics” section on page 5-30.

## Interactions and Restrictions

The following sections describe the interactions and restrictions for directed call park:
- **Interactions, page 5-20**
- **Restrictions, page 5-22**

### Interactions

The following sections describe how directed call park interacts with Cisco Unified Communications Manager applications and call processing:
- **Music On Hold, page 5-21**
- **Route Plan Report, page 5-21**
- **Calling Search Space and Partitions, page 5-21**
- **Immediate Divert, page 5-21**
Music On Hold

Music on hold allows users to place calls on hold with music that is provided from a streaming source. Music on hold allows two types of hold:

- **User hold**—The system invokes this type of hold when a user presses the Hold button or Hold softkey.
- **Network hold**—This type of hold takes place when a user activates the transfer, conference, or call park feature, and the hold automatically gets invoked. This hold type applies to directed call park because directed call park is a transfer function.

Route Plan Report

The route plan report displays the patterns and directory numbers that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to directed call park. See the Route Plan Report chapter in the *Cisco Unified Communications Manager Administration Guide*.

Calling Search Space and Partitions

Assign the directed call park directory number or range to a partition to limit directed call park access to users on the basis of the device calling search space. See Calling Search Space Configuration and Partition Configuration in the *Cisco Unified Communications Manager Administration Guide*.

Immediate Divert

Directed call park supports Immediate Divert (iDivert or Divert softkey). For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to a voice-messaging mailbox by pressing the iDivert or Divert softkey. User A receives the voice-messaging mailbox greeting of user B.

Barge

The following paragraphs describe the differences between Barge and cBarge with directed call park.

**Barge with Directed Call Park**

The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggyback” on the target phone. The target phone includes most of the common features, even when the target is being barged; therefore, the barge initiator has no feature access. When the target parks a call by using directed call park, the barge initiator then must release its call (the barge).

**cBarge with Directed Call Park**

The target and barge initiator act as peers. The cBarge feature uses a conference bridge that makes it behave similar to a meet-me conference. Both phones (target and barge initiator) retain full access to their features.
Call Park

Cisco recommends that you do not configure both directed call park and the Park softkey for call park, but the possibility exists to configure both. If you configure both, ensure that the call park and directed call park numbers do not overlap.

A caller who has been parked (the parkee) by using the directed call park feature cannot, while parked, use the standard call park feature.

Restrictions

The following restrictions apply to directed call park:

- Cisco Unified Communications Manager can park only one call at each directed call park number.
- Ensure each directed call park directory number, partition, and range is unique within the Cisco Unified Communications Manager cluster. If the Park softkey is also activated (not recommended), ensure that no overlap exists between call park numbers and directed call park numbers.
- A caller who has been parked (the parkee) by using the directed call park feature cannot, while parked, use the standard call park feature.
- The directed call park BLF cannot monitor a range of directed call park numbers. A user can monitor only individual directed call park numbers by using the directed call park BLF. For example, if you configure a directed call park number range 8X, you cannot use the directed call park BLF to monitor that whole range of 80 to 89.
- You cannot delete a directed call park number that a device is configured to monitor (using the BLF button). A message indicates that the directed call park number or range cannot be deleted because it is in use. To determine which devices are using the number, click the Dependency Records link on the Directed Call Park Configuration window.
- If reversion number is not configured, the call reverts to the parker (parking party) after the call park reversion timer expires. Directed Call Park for phones that are running SIP is designed as busy lamp field (BLF) plus call transfer (to a park code). The transfer functionality remains the same as for phones that are running SCCP. The following limitations apply to directed call park for phones that are running SIP:
  - Directed call park gets invoked by using the transfer softkey on Cisco Unified IP Phones 7940 and 7960 that are running SIP.
  - The system does not support directed call park when the blind transfer softkey is used on Cisco Unified IP Phones 7940 and 7960 that are running SIP.
  - The system does not support directed call park BLF on Cisco Unified IP Phones 7940 and 7960 that are running SIP, and third-party phones that are running SIP.

See the “Configuring a Directed Call Park Number” section on page 5-24 for configuration details.

Additional Information

See the “Related Topics” section on page 5-30.
Installing and Activating Directed Call Park

Directed call park system feature comes standard with Cisco Unified Communications Manager software. Any phone that can perform a transfer can use directed call park. It does not require special installation. Cisco recommends that you configure either call park or directed call park, but not both. If you do configure both, ensure that the directed call park and call park numbers do not overlap.

Additional Information
See the “Related Topics” section on page 5-30.

Configuring Directed Call Park

This section contains the following information:

- Setting the Service Parameters for Directed Call Park, page 5-23
- Finding a Directed Call Park Number, page 5-23
- Configuring a Directed Call Park Number, page 5-24
- Directed Call Park Configuration Settings, page 5-25
- Configuring BLF/Directed Call Park Buttons, page 5-27
- BLF/Directed Call Park Configuration Settings, page 5-27
- Synchronizing Directed Call Park With Affected Devices, page 5-28
- Deleting a Directed Call Park Number, page 5-29

Tip
Before you configure directed call park, review the “Directed Call Park Configuration Checklist” section on page 5-3.

Setting the Service Parameters for Directed Call Park

The Call Park Reversion Timer clusterwide service parameter affects directed call park. This parameter determines the time that a call remains parked. The default specifies 60 seconds. When the timer expires, the parked call returns to either the device that parked the call or to another specified number, depending on what you configure in the Directed Call Park Configuration window.

Additional Information
See the “Related Topics” section on page 5-30.

Finding a Directed Call Park Number

Because you may have several directed call park numbers in your network, Cisco Unified Communications Manager lets you locate specific directed call park numbers on the basis of specific criteria. Use the following procedure to locate directed call park numbers.
Procedure

Step 1  Choose Call Routing > Directed Call Park.

The Find and List Directed Call Parks window displays.

Step 2  To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records:
- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

Note  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Related Topics” section on page 5-30.

Configuring a Directed Call Park Number

This section describes how to add, copy, and update a single directed call park extension number or range of extension numbers.
Chapter 5  Call Park and Directed Call Park  

Configuring Directed Call Park

Procedure

Step 1  Choose **Call Routing > Directed Call Park**.

Step 2  Perform one of the following tasks:

- To add a new Directed Call Park Number, click **Add New**.
- To copy a Directed Call Park Number, use the procedure in the “Finding a Directed Call Park Number” section on page 5-23 to locate the directed call park number or range of numbers. Click the Copy icon.
- To update a Directed Call Park Number, use the procedure in the “Finding a Directed Call Park Number” section on page 5-23 to locate the directed call park number or range of numbers.

The Directed Call Park Number Configuration window displays.

Step 3  Enter or update the appropriate settings as described in **Table 5-6**.

Step 4  To save the new or changed call park numbers in the database, click **Save**.

**Note**

- If you update a directed call park number, Cisco Unified Communications Manager reverts any call that is parked on that number only after the Call Park Reversion Timer expires.

- Whenever changes are made to directed call park numbers or ranges, any devices that are configured to monitor those directed call park numbers by using the BLF must restart to correct the display. Change notification automatically restarts impacted devices when it detects directed call park number changes. You can also use the Restart Devices button on the Directed Call Park Configuration window.

**Additional Information**

See the “Related Topics” section on page 5-30.

Directed Call Park Configuration Settings

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. Configured directed call park numbers exist clusterwide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number. See **Interactions and Restrictions, page 5-20**, for a list of the phone models that support the BLF.

Cisco Unified Communications Manager can park only one call at each directed call park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the directed call park number at which the call is parked. Configure the retrieval prefix in the Directed Call Park Configuration window.

**Table 5-2** provides a checklist to configure directed call park. For more information on directed call park, see the “**Introducing Directed Call Park**” section on page 5-19 and the “**Related Topics**” section on page 5-30.

**Table 5-6** describes the directed call park configuration settings.
Chapter 5 Call Park and Directed Call Park

Configuring Directed Call Park

Table 5-6 Directed Call Park Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Enter the directed call park number. You can enter literal digits or the wildcard character X (the system allows one or two Xs). For example, enter 5555 to define a single call park number of 5555 or enter 55XX to define a range of directed call park extension numbers from 5500 to 5599. Make sure that the directed call park numbers are unique and that they do not overlap with call park numbers.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a brief description of this directed call park number or range. The description can include up to 50 characters in any language, but it cannot include double-quotes (“”), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Partition</td>
<td>If you want to use a partition to restrict access to the directed call park numbers, choose the desired partition from the drop-down list box. If you do not want to restrict access to the directed call park numbers, leave the partition as the default of &lt;None&gt;. See Searching for a Partition in the Cisco Unified Communications Manager Administration Guide for instructions on finding a partition when there are a large number of them configured. Make sure that the combination of directed call park number and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Reversion Number</td>
<td>Enter the number to which you want the parked call to return if not retrieved, or leave the field blank. A reversion number can comprise digits only; you cannot use wildcards.</td>
</tr>
<tr>
<td>Reversion Calling Search Space</td>
<td>Using the drop-down list box, choose the calling search space or leave the calling search space as the default of &lt;None&gt;.</td>
</tr>
<tr>
<td>Retrieval Prefix</td>
<td>For this required field, enter the prefix for retrieving a parked call. The system needs the retrieval prefix to distinguish between an attempt to retrieve a parked call and an attempt to initiate a directed park.</td>
</tr>
</tbody>
</table>

Note Whenever changes are made to directed call park numbers, any devices that are configured to monitor those directed call park numbers by using the directed call BLF must restart to correct the display. Change notification automatically restarts impacted devices when it detects directed call park number changes. You also can use the Restart Devices button on the Directed Call Park Configuration window.

Additional Information
See the “Related Topics” section on page 5-30.
Configuring BLF/Directed Call Park Buttons

To configure BLF/Directed Call Park buttons, perform the following procedure:

Procedure

Step 1  To configure the BLF/Directed Call Park button in the Phone Configuration window, find the phone, as described in the “Cisco Unified IP Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

Step 2  To configure the BLF/Directed Call Park button for user device profiles, find the user device profile as described in the “Device Profile Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

Step 3  After the configuration window displays, click the Add a new BLF Directed Call Park link in the Association Information pane.

Tip  The link does not display in the Association Information pane if the phone button template that you applied to the phone or device profile does not support BLF/Directed Call Park.

Step 4  Configure the settings, as described in Table 5-7.

Step 5  After you complete the configuration, click Save and close the window.

The directory number(s) display in the Association Information pane of the Phone Configuration Window.

Additional Information

See the “Related Topics” section on page 5-30.

BLF/Directed Call Park Configuration Settings

Table 5-7 describes the settings that you configure for BLF/Directed Call Park buttons.

Table 5-7  BLF/Directed Call Park Button Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number</td>
<td>The Directory Number drop-down list box displays a list of directory numbers that exist in the Cisco Unified Communications Manager database.</td>
</tr>
<tr>
<td></td>
<td>For phones that are running SCCP or phones that are running SIP, choose the number (and corresponding partition, if it displays) that you want the system to dial when the user presses the speed-dial button; for example, 6002 in 3. Directory numbers that display without specific partitions belong to the default partition.</td>
</tr>
</tbody>
</table>
Configuring Directed Call Park

Synchronizing Directed Call Park With Affected Devices

To synchronize devices with directed call park information that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose Call Routing > Directed Call Park.

The Find and List Directed Call Parks window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.

The window displays a list of directed call parks that match the search criteria.

Step 4 Click the directed call park to which you want to synchronize applicable devices. The Directed Call Park Configuration window displays.

Step 5 Make any additional configuration changes.

Step 6 Click Save.

Step 7 Click Apply Config.

The Apply Configuration Information dialog displays.

Step 8 Click OK.

Additional Information

See the “Related Topics” section on page 5-30.
Deleting a Directed Call Park Number

This section describes how to delete directed call park numbers from the Cisco Unified Communications Manager database.

Procedure

1. Step 1  Using the procedure in the “Finding a Directed Call Park Number” section on page 5-23, locate the directed call park number or range of numbers.
2. Step 2  Click the directed call park number or range of numbers that you want to delete.
3. Step 3  Click **Delete**.

Note
Deleting a directed call park number causes Cisco Unified Communications Manager to immediately revert any call that is parked on that number. This occurs because, when the number is deleted, a parked call on that number cannot remain parked or be retrieved in the usual way and must be reverted.

Note
You cannot delete a directed call park number that a device is configured to monitor (using the BLF button). A message indicates that the directed call park number cannot be deleted because it is in use. To determine which devices are using the number, click the Dependency Records link in the Directed Call Park Configuration window.

Additional Information
See the “Related Topics” section on page 5-30.

Assisted Directed Call Park for Cisco Unified IP Phones (SIP)

Assisted directed call park is supported on all Cisco Unified IP Phones 7900, 8900, and 9900 series that support SIP. With assisted directed call park, the end user needs to press only one button to direct-park a call. You must configure a BLF Directed Call Park button. Then, when the user presses an idle BLF Directed Call Park feature button for an active call, the active call gets parked immediately at the Dpark slot that associates with the Directed Call Park feature button.

Additional Information
See the following sections:

- Configuring BLF/Directed Call Park Buttons, page 5-27
- Related Topics, page 5-30
Related Topics

Call Park
- Call Park Configuration Checklist, page 5-2
- Introducing Call Park, page 5-4
- System Requirements for Call Park, page 5-7
- Interactions and Restrictions, page 5-8
- Installing and Activating Call Park, page 5-10
- Configuring Call Park, page 5-11
- Setting the Service Parameters for Call Park, page 5-11
- Finding a Call Park Number, page 5-11
- Configuring a Call Park Number, page 5-13
- Call Park Configuration Settings, page 5-13
- Synchronizing Directed Call Park With Affected Devices, page 5-28
- Deleting a Call Park Number, page 5-15

Park Monitoring (Cisco Unified IP Phones 8961, 9951, and 9971 only)
- Park Monitoring for Cisco Unified IP Phones 8961, 9951, and 9971, page 5-16

Directed Call Park
- Directed Call Park Configuration Checklist, page 5-3
- Introducing Directed Call Park, page 5-19
- System Requirements for Directed Call Park, page 5-20
- Interactions and Restrictions, page 5-20
- Installing and Activating Directed Call Park, page 5-23
- Setting the Service Parameters for Directed Call Park, page 5-23
- Finding a Directed Call Park Number, page 5-23
- Configuring a Directed Call Park Number, page 5-24
- Directed Call Park Configuration Settings, page 5-25
- Configuring BLF/Directed Call Park Buttons, page 5-27
- BLF/Directed Call Park Configuration Settings, page 5-27
- Synchronizing Directed Call Park With Affected Devices, page 5-28
- Deleting a Directed Call Park Number, page 5-29

Assisted Directed Call Park (Cisco Unified IP Phones 8961, 9951, and 9971 only)
- Assisted Directed Call Park for Cisco Unified IP Phones (SIP), page 5-29
Additional Information

- Phone Button Template Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Partition Configuration, Cisco Unified Communications Manager Administration Guide
- Media Termination Point Configuration, Cisco Unified Communications Manager Administration Guide
- Route Plan Report, Cisco Unified Communications Manager Administration Guide
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- End User Configuration, Cisco Unified Communications Manager Administration Guide
- User Group Configuration, Cisco Unified Communications Manager Administration Guide
- Clustering, Cisco Unified Communications Manager System Guide
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone user documentation and release notes (all models)
CHAPTER 6

Call Pickup

The Call Pickup features allow users to answer calls that come in on a directory number other than their own. The “Introducing Call Pickup” section on page 6-10 describes these features.

This section covers the following topics:

- Configuration Checklist for Call Pickup and Group Call Pickup, page 6-1
- Configuration Checklist for Other Group Pickup, page 6-3
- Configuration Checklist for Directed Call Pickup, page 6-5
- Configuration Checklist for BLF Call Pickup, page 6-7
- Introducing Call Pickup, page 6-10
- System Requirements for Call Pickup, page 6-22
- Interactions and Restrictions, page 6-23
- Installing and Activating Call Pickup, page 6-25
- Configuring Call Pickup Features, page 6-26
- Configuring Call Pickup Groups, page 6-27
- Related Topics, page 6-34

Configuration Checklist for Call Pickup and Group Call Pickup

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey, PickUp, for this type of call pickup.

Note

Cisco Unified IP Phone 6900 uses the Call Pickup programmable feature button or the Call Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Call Pickup programmable feature button.

The Group Call Pickup feature allows users to pick up incoming calls in another group. Users must dial the appropriate call pickup group number when this feature is activated from a Cisco Unified IP Phone. Use the softkey, GPickUp, for this type of call pickup.

Note

Cisco Unified IP Phone 6900 uses the Group Pickup programmable feature button or the Group Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Group Pickup programmable feature button.
When the user invokes the Group Call Pickup phone feature while multiple calls are incoming to a pickup group, the user gets connected to the incoming call that has been ringing the longest.

**Note**
The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

Table 6-1 provides a checklist to configure Call Pickup and Group Call Pickup features. For more information on these features, see the “Introducing Call Pickup” section on page 6-10 and the “Related Topics” section on page 6-34.

<table>
<thead>
<tr>
<th>Table 6-1 Call Pickup and Group Call Pickup Configuration Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Steps</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. The Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user activates this feature from a Cisco Unified IP Phone. Use the softkey, OPickUp, for this type of call pickup.

**Note**
Cisco Unified IP Phone 6900 uses the Other Pickup programmable feature button or the Other Pickup softkey; Cisco Unified IP Phone 8900 and 9900 use only the Other Pickup programmable feature button.

When more than one associated group exists, the priority of answering calls for the associated group goes from the first associated group to the last associated group. For example, groups A, B, and C associate with group X, and the priority of answering calls goes to group A, B, and then C. First, group X picks up incoming call in group A, though a call may have come in earlier in group C than the incoming call in group A.
Note: Usually, within the same group, the longest alerting call (longest ringing time) gets picked up first if multiple incoming calls occur in that group. For other group call pickup, priority takes precedence over the ringing time if multiple associated pickup groups are configured.

Table 6-2 provides a checklist to configure other group pickup. For more information on other group pickup, see the “Introducing Call Pickup” section on page 6-10 and the “Related Topics” section on page 6-34.

### Table 6-2 Other Group Pickup Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure a list of associated groups that can be chosen from all pickup groups. The list can include up to 10 groups.</td>
</tr>
<tr>
<td></td>
<td>Defining a Pickup Group for Other Group Pickup, page 6-33</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Calling Search Space and TOD parameters for members of the associated groups to your group.</td>
</tr>
<tr>
<td></td>
<td>Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Time-of-Day Routing, CiscoUnified Communications Manager System Guide</td>
</tr>
<tr>
<td></td>
<td>Time Schedule Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Time Period Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>If you want automatic call answering for other group call pickup, enable the Auto Call Pickup Enabled service parameter by entering the value True. The default specifies False.</td>
</tr>
<tr>
<td></td>
<td>Auto Call Pickup, page 6-17.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>If the Auto Call Pickup Enabled service parameter is False, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the time that a call takes to get restored if a call is picked up but not answered by other group call pickup.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enter a value for the service parameter Pickup Locating Timer. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
Chapter 6  Call Pickup

Configuration Checklist for Directed Call Pickup

Table 6-2  Other Group Pickup Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Assigning Softkey Templates to IP Phones</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td>To configure the Other Pickup (OPickUp) softkey for the phone, modify and add the Standard User or Standard Feature softkey template to the phone. Modify the template to include the OPickUp softkey by using the following steps.</td>
<td></td>
</tr>
<tr>
<td>• Choose Device &gt; Device Settings &gt; Softkey Template in Cisco Unified Communications Manager Administration.</td>
<td></td>
</tr>
<tr>
<td>• Choose the desired softkey template.</td>
<td></td>
</tr>
<tr>
<td>• Choose the Softkey Layout Configuration link.</td>
<td></td>
</tr>
<tr>
<td>• Choose On Hook or Off Hook call states.</td>
<td></td>
</tr>
<tr>
<td>• Choose Other Pickup (OPickUp) in the Unselected Softkeys box. Click the right arrow to move the Other Pickup (OPickup) softkey to the Selected Softkeys box.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To restrict calls to be picked up by a phone within only its own group, deny the OPickUp softkey in the softkey template.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Phone Button Template Configuration Settings</strong>, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td>Add the OPickup button to the phone button templates, if needed.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>See the phone documentation for instructions on how users access the Other Group Pickup feature on their Cisco Unified IP Phone.</strong></td>
</tr>
<tr>
<td>Notify users that the Other Group Pickup feature is available.</td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Checklist for Directed Call Pickup

The Directed Call Pickup feature allows a user to pick up a ringing call on a DN directly by pressing the GPickUp or Group Pickup softkeys and entering the directory number of the device that is ringing. Cisco Unified Communications Manager uses the associated group mechanism to control the privilege of a user who wants to pick up an incoming call by using Directed Call Pickup. The associated group of a user specifies one or more call pickup groups that have been associated to the pickup group to which the user belongs.

If a user wants to pick up a ringing call from a DN directly, the associated groups of the user must contain the pickup group to which the DN belongs. If two users belong to two different call pickup groups and the associated groups of the users do not contain the call pickup group of the other user, the users cannot invoke Directed Call Pickup to pick up calls from each other.

When the user invokes the Directed Call Pickup feature and enters a DN from which to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest ringing call in the call pickup group to which the DN belongs.

If multiple calls are ringing on a particular DN and the user invokes Directed Call Pickup to pick up a call from the DN, the user connects to the incoming call that has been ringing the specified DN the longest.
Table 6-3 provides a checklist to configure directed call pickup. For more information on directed call pickup, see the “Introducing Call Pickup” section on page 6-10 and the “Related Topics” section on page 6-34.

Table 6-3  Directed Call Pickup Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Define a list of associated groups that can be chosen from all pickup groups. The list can include up to 10 groups.</td>
</tr>
<tr>
<td></td>
<td>Related Procedures and Topics</td>
</tr>
<tr>
<td></td>
<td>Defining a Pickup Group for Other Group Pickup, page 6-33</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure Calling Search Space and TOD parameters for members of the associated groups to your group.</td>
</tr>
<tr>
<td></td>
<td>Related Procedures and Topics</td>
</tr>
<tr>
<td></td>
<td>Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Time-of-Day Routing, Cisco Unified Communications Manager System Guide</td>
</tr>
<tr>
<td></td>
<td>Time Schedule Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Time Period Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 3</td>
<td>If you want automatic call answering for directed call pickup, enable the Auto Call Pickup Enabled service parameter by entering the value True. The default specifies False.</td>
</tr>
<tr>
<td></td>
<td>Related Procedures and Topics</td>
</tr>
<tr>
<td></td>
<td>Auto Call Pickup, page 6-17.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 4</td>
<td>If the Auto Call Pickup Enabled service parameter is False, enter a value for the Call Pickup No Answer Timer service parameter. This parameter controls the time that a call takes to get restored if a call is picked up but not answered by directed call pickup.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a value for the service parameter Pickup Locating Timer. This parameter controls the time for call selection for call pickup, group call pickup, and other group call pickup.</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
You can associate the busy lamp field (BLF) button on a Cisco Unified IP Phone to a DN. This allows Cisco Unified Communications Manager to notify a phone user when a call is waiting to be picked up from the DN. The DN represents the BLF DN, and the phone that picks up the call to the BLF DN represents the BLF call pickup initiator.

The following rules apply to the BLF DN and the BLF call pickup initiator:

- The BLF call pickup initiator gets selected as the next available line or as a specified line. To use a specified line, the line must remain off hook before the BLF SD button is pressed.
- You can configure a hunt list member DN as the BLF DN to allow an incoming call to a hunt list member to be picked up by the BLF call pickup initiator. The incoming call on the hunt list member can come from the hunt list or be a directed call. The behavior in each case depends on how call pickup is configured for the hunt list member DN, the BLF DN, and the hunt pilot number.
- When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the phone must remain off hook or the user must press the answer key to pick up the call.

The BLF SD button on the phone can exist in any of the following states:

- Idle—Indicates that no call exists on the BLF DN.

### Configuration Checklist for BLF Call Pickup

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>To configure the Group Call Pickup (GPickUp) softkey for the phone, modify and add the Standard User or Standard Feature softkey template to the phone. Modify the template to include the GPickUp softkey with the following steps.</td>
</tr>
<tr>
<td></td>
<td>Choose Device &gt; Device Settings &gt; Softkey Template in Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td></td>
<td>Choose the desired softkey template.</td>
</tr>
<tr>
<td></td>
<td>Choose the Softkey Layout Configuration link.</td>
</tr>
<tr>
<td></td>
<td>Choose On Hook or Off Hook call states.</td>
</tr>
<tr>
<td></td>
<td>Choose Group Call Pickup(GPickUp) in the Unselected Softkeys box. Click the right arrow to move the Group Call Pickup (GPickUp) softkey to the Selected Softkeys box.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To restrict calls to be picked up by phones only within its own group, deny the GPickUp softkey in the softkey template.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Add the Group Pickup button to the phone button templates, if needed.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Notify users that the Directed Call Pickup feature is available.</td>
</tr>
</tbody>
</table>
 Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communications Manager

Chapter 6      Call Pickup

Configuration Checklist for BLF Call Pickup

- Busy—Indicates that at least one active call exists on the BLF DN, but no alerts exist.
- Alert—Indicates by flashing that at least one incoming call exists on the BLF DN.

Note: You can optionally configure an audible alert in addition to the visual alert.

The following actions take place for an incoming call to the BLF DN:

1. The BLF SD button flashes on the BLF call pickup initiator phone to indicate that an incoming call to the BLF DN exists.
2. If auto call pickup is configured, the user presses the BLF SD button on the call pickup initiator phone to pick up the incoming call. If auto call pickup is not configured, the phone must remain off hook, or the user must press the answer key to pick up the call.

Table 6-4 provides a checklist to configure BLF call pickup. For more information on BLF call pickup, see the “Introducing Call Pickup” section on page 6-10 and the “Related Topics” section on page 6-34.

Table 6-4 BLF Call Pickup Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Configure a call pickup group for the BLF DN. Make sure that the name and number are unique.</td>
<td>Configuring a Call Pickup Group, page 6-28</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Create another call pickup group and associate it to the call pickup group that was created in Step 1. You can associate a call pickup group to multiple BLF DN call pickup groups.</td>
<td></td>
</tr>
<tr>
<td>Only directory numbers that are assigned to a call pickup group can use the BLF Call Pickup feature.</td>
<td></td>
</tr>
<tr>
<td>If partitions are used with call pickup numbers, make sure that the directory numbers that are assigned to the call pickup group have a calling search space that includes the appropriate partitions.</td>
<td></td>
</tr>
<tr>
<td>Note: You do not always need to create another call pickup group. A pickup group can have itself as its association group.</td>
<td>Configuring a Call Pickup Group, page 6-28</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Create a customized phone button template that contains the Speed Dial BLF button and associate that phone button template with the phone devices that will be used to pick up calls from the BLF DN. The phone that picks up calls from the BLF DN represents the call pickup initiator.</td>
<td>Phone Button Template Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
Table 6-4  BLF Call Pickup Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
</table>
| Step 4             | Configure the BLF SD number on the phone that you created for the BLF call pickup initiator. To do this, click the Add a new BLF SD link in the Phone Configuration window. The Busy Lamp Field SpeedDial Configuration window displays. Select a directory number as the BLF DN to be monitored by the BLF SD button. Use the Call Pickup check box to enable the pickup feature that is associated with the BLF SD button.  
**Note** If the check box is checked, you can use the BLF SD button for BLF call pickup and BLF speed dial. If the check box is not checked, you can use the BLF SD button only for BLF speed dial. | Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide |
| Step 5             | In the Directory Number Configuration window, add the DN that is used as the BLF call pickup initiator to the call pickup group that was created in Step 2.  
**Note** The pickup group for the BLF DN should belong to the association groups for the initiator. The pickup group created in Step 2 must include the pickup group created in Step 1 in its set of association groups. | Directory Number Configuration Settings, Cisco Unified Communications Manager Administration Guide |
| Step 6             | In the Directory Number Configuration window, add the BLF DN to the call pickup group that was created in Step 1. | Directory Number Configuration Settings, Cisco Unified Communications Manager Administration Guide |
| Step 7             | (Optional) In the Service Parameter Configuration window, enable the following Cisco CallManager service parameters to activate BLF call pickup audio alerting for the cluster:  
* BLF Pickup Audio Alert Setting of Idle Station  
* BLF Pickup Audio Alert Setting of Busy Station | Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide |
| Step 8             | (Optional) To enable the BLF call pickup initiator to connect to a caller by pressing the BLF-SD, set the Cisco CallManager service parameter Auto Call Pickup Enabled to true.  
If you set this service parameter to false, the call pickup initiator must press the BLF-SD button as well as go offhook or press the answer button to answer the call. | Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide |
| Step 9             | (Optional) In the Phone Configuration window, enable the following fields to activate BLF call pickup audio alerting for the BLF call pickup initiator:  
* BLF Audible Alert Setting (Phone Idle)  
* BLF Audible Alert Setting (Phone Busy) | Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide |
Introducing Call Pickup

Cisco Unified IP Phones support the following types of call pickup: call pickup, group call pickup, other group pickup, directed call pickup, BLF call pickup, and auto call pickup.

The following information applies to all of the call pickup types:

- Both idle and offhook call states make the three softkeys, PickUp, GPickUp, and OPickUp, available. The administrator must modify the standard softkey template to include these softkeys for the users to invoke the Call Pickup features. See the “Configuration Checklist for Call Pickup and Group Call Pickup” section on page 6-1, the “Configuration Checklist for Other Group Pickup” section on page 6-3, and the “Configuration Checklist for Directed Call Pickup” section on page 6-5.

- If a user invokes call pickup to pick up a call from a phone that has no incoming calls, the user receives a “No Call(s) for Pickup” message. If a user invokes call pickup to pick up a ringing call from a DN for which the user is not configured to pick up calls, the user receives reorder tone.

- Call Pickup operates with a consult transfer call. The following scenario provides an example. User A calls user C, and user C answers. User C presses the Transfer key and dials phone D. User E hears phone D ring and uses call pickup to pick up the call that is ringing on phone D. After user C presses the Transfer key again, user A and user E connect. Call Pickup also functions if user C presses Transfer before either phone D picks up the call or user E invokes Call Pickup.

- The Call Pickup feature operates with ad hoc conference calls. The following scenario provides an example. User A calls user C, and user C answers. User C presses the Conf key and makes a consultation call to phone D. User E hears phone D ring and uses call pickup to pick up the call that is ringing on phone D. User C then presses the Conf key again, and user A, user C, and user E connect to an ad hoc conference. Call pickup also functions if user C presses the Conf key a second time before user E picks up the call that is ringing on phone D.

- If user E successfully invokes call pickup to pick up a call from user A that is ringing on DN C while the Auto Call Pickup Enabled service parameter is set to False, but user E then does not pick up the call before the time that is specified in the Call Pickup No Answer Timer expires, the original call from user A gets restored and continues to ring at DN C.

- A user can only invoke Call Pickup if the user has a line free to pick up the call. If the user lines are busy with held calls, the user receives a “No Line Available for Pickup” message on the display and the original call continues to ring at the called number.
For details about each of the types of call pickup, see the following topics:

- Call Pickup, page 6-11
- Group Call Pickup, page 6-11
- Other Group Pickup, page 6-12
- Directed Call Pickup, page 6-12
- Busy Lamp Field Call Pickup, page 6-16
- Auto Call Pickup, page 6-17

Additional Information
See the “Related Topics” section on page 6-34.

**Call Pickup**

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey or feature button, PickUp, for this type of call pickup.

The Call Pickup feature functions whether auto call pickup is enabled or not. See the “Auto Call Pickup” section on page 6-17 for details.

Additional Information
See the “Related Topics” section on page 6-34.

**Group Call Pickup**

The Group Call Pickup feature allows users to pick up incoming calls in another group. User must dial the appropriate call pickup group number when this feature is activated from a Cisco Unified IP Phone. Use the softkey, GPickUp, or the feature button, Group Pickup, for this type of call pickup.

When the user invokes the Group Call Pickup phone feature while multiple calls are incoming to a pickup group, the user gets connected to the incoming call that has been ringing the longest.

**Note**

The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

The Group Call Pickup feature functions whether auto call pickup is enabled or not. See the “Auto Call Pickup” section on page 6-17 for details.

Additional Information
See the “Related Topics” section on page 6-34.
Other Group Pickup

The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. The Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user activates this feature from a Cisco Unified IP Phone. Use the softkey or feature button, OPickUp, for this type of call pickup.

When more than one associated group exists, the priority of answering calls for the associated group goes from the first associated group to the last associated group. For example, groups A, B, and C associate with group X, and the priority of answering calls goes to group A, B, and then C. First, group X picks up incoming call in group A, though a call may have come in earlier in group C than the incoming call in group A.

Note

Usually, within the same group, the longest alerting call (longest ringing time) gets picked up first if multiple incoming calls occur in that group. For other group call pickup, priority takes precedence over the ringing time if multiple associated pickup groups are configured.

The Other Group Pickup feature functions whether auto call pickup is enabled or not. See the “Auto Call Pickup” section on page 6-17 for details.

Additional Information

See the “Related Topics” section on page 6-34.

Directed Call Pickup

The Directed Call Pickup feature allows a user to pick up a ringing call on a DN directly by pressing the GPickUp softkey or Group Pickup feature button and entering the directory number of the device that is ringing. Cisco Unified Communications Manager uses the associated group mechanism to control the privilege of a user who wants to pick up an incoming call by using Directed Call Pickup. The associated group of a user specifies one or more call pickup groups that have been associated to the pickup group to which the user belongs.

If a user wants to pick up a ringing call from a DN directly, the associated groups of the user must contain the pickup group to which the DN belongs. If two users belong to two different call pickup groups and the associated groups of the users do not contain the call pickup group of the other user, the users cannot invoke Directed Call Pickup to pick up calls from each other.

When the user invokes the Directed Call Pickup feature and enters a DN from which to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest ringing call in the call pickup group to which the DN belongs.

If multiple calls are ringing on a particular DN and the user invokes Directed Call Pickup to pick up a call from the DN, the user connects to the incoming call that has been ringing the specified DN the longest.

The Directed Call Pickup feature functions whether auto call pickup is enabled or not. See the “Auto Call Pickup” section on page 6-17 for details.

Additional Information

See the “Related Topics” section on page 6-34.
Examples of Directed Call Pickup

The following examples illustrate various Directed Call Pickup scenarios.

Basic Directed Call Pickup

This scenario illustrates Directed Call Pickup. The following setup takes place, as shown in Figure 6-1:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups such that its Other Pickup Groups specify 111 and 333.
3. DN of phone C specifies 1000 in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.

5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.
7. Phone A and phone E connect, and phone C stops ringing.

Figure 6-2 shows the connection state between phone A and phone E after Directed Call Pickup completes.

Directed Call Pickup Control Mechanism—Reject Example 1

This scenario illustrates the control mechanism that causes rejection of a Directed Call Pickup attempt. The following setup takes place, as shown in Figure 6-3:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association group 333.
3. DN of phone C specifies 1000 in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.

Figure 6-3 Directed Call Pickup Setup 1 That Leads to Rejection

5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.
7. The Directed Call Pickup attempt for phone E gets rejected because the pickup group of phone E, 222, does not have group 111 in its association list.

Figure 6-4 shows the connection state between phone A and phone E after Directed Call Pickup fails.

Figure 6-4 Directed Call Pickup Gets Rejected, Example 1

Directed Call Pickup Control Mechanism—Reject Example 2
This scenario illustrates the control mechanism that causes rejection of a Directed Call Pickup attempt. The following setup takes place, as shown in Figure 6-5:
1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups 111 and 333.
3. DN of phone C specifies PT_C/1000 in pickup group 111, and PT_C specifies the partition of phone C.
4. DN of phone E specifies PT_E/2000 in pickup group 222, PT_E specifies the partition of phone E, and the Calling Search Space (CSS) of phone E specifies PT_E.
5. User A calls phone C, and phone C begins to ring.
6. User E presses the GPickUp softkey and enters DN of phone C, which is 1000.
7. The Directed Call Pickup attempt for phone E gets rejected because the CSS of phone E does not contain the partition of phone C.

Figure 6-6 shows the connected state between phone A and phone E after Directed Call Pickup fails.

**Directed Call Pickup Control Mechanism—Multiple Calls**

This scenario illustrates Directed Call Pickup when multiple calls are available for pickup. The following setup takes place, as shown in Figure 6-7:

1. Three pickup groups that are created comprise group numbers 111, 222, and 333.
2. Pickup group 222 includes association groups 111 and 333.
3. DN of phone C specifies 1000, DN of phone D specifies 3000, and both phones reside in pickup group 111.
4. DN of phone E specifies 2000 in pickup group 222.
Introducing Call Pickup

Figure 6-7 Directed Call Pickup Setup With Multiple Calls

5. User A calls phone C, and user B calls phone D. Phone C and phone D begin to ring.
6. User E presses the GPickUp softkey and enters DN of phone D, which is 3000.
7. Phone B and phone E connect, and phone D stops ringing.

Figure 6-8 shows the connection state between phone B and phone E after Directed Call Pickup completes.

Figure 6-8 Directed Call Pickup With Multiple Calls Completes

Busy Lamp Field Call Pickup

You can associate the busy lamp field (BLF) button on a Cisco Unified IP Phone to a DN. This allows Cisco Unified Communications Manager to notify a phone user when a call is waiting to be picked up from the DN. The DN represents the BLF DN, and the phone that picks up the call to the BLF DN represents the BLF call pickup initiator.

The following rules apply to the BLF DN and the BLF call pickup initiator:

- The BLF call pickup initiator gets selected as the next available line or as a specified line. To use a specified line, the line must remain off hook before the BLF SD button is pressed.
- You can configure a hunt list member DN as the BLF DN to allow an incoming call to a hunt list member to be picked up by the BLF call pickup initiator. The incoming call on the hunt list member can come from the hunt list or be a directed call. The behavior in each case depends on how call pickup is configured for the hunt list member DN, the BLF DN, and the hunt pilot number.
When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the phone must remain off hook or the user must press the answer key to pick up the call.

The BLF SD button on the phone can exist in any of the following states:

- Idle—Indicates that no call exists on the BLF DN.
- Busy—Indicates that at least one active call exists on the BLF DN, but no alerts exist.
- Alert—Indicates by flashing that at least one incoming call exists on the BLF DN.

Note: You can optionally configure an audible alert in addition to the visual alert.

The following actions take place for an incoming call to the BLF DN:

1. The BLF SD button flashes on the BLF call pickup initiator phone to indicate that an incoming call to the BLF DN exists.
2. If auto call pickup is configured, the user presses the BLF SD button on the call pickup initiator phone to pick up the incoming call. If auto call pickup is not configured, the phone must remain off hook, or the user must press the answer key to pick up the call.

**BLF Call Pickup Example**

This scenario illustrates BLF call pickup. The following elements are configured:

- Group 111 represents a call pickup group that includes the BLF DN (phone B), an outside phone (phone A), and other phones.
- Group 222 represents a call pickup group that is associated to Group 111. Group 222 includes phone C.
- Phone A represents an outside phone.
- Phone B represents the BLF DN phone in Group 111.
- Phone C represents a user phone in Group 222 that has the BLF SD button configured to monitor the phone B BLF DN and has call pickup enabled. It represents the BLF call pickup initiator phone.

When a call from phone A comes in to phone B, the BLF SD button on phone C lights. The user at phone C presses the button and connects to the phone A caller.

If a hunt list pilot number is configured as part of Group 111, a call from phone A to the hunt group causes the BLF SD button on phone C to light, and the user at phone C can press the button to connect to the caller at phone A.

**Additional Information**

See the “Related Topics” section on page 6-34.

**Auto Call Pickup**

You can automate call pickup, group pickup, other group pickup, directed call pickup, and BLF call pickup by enabling the Auto Call Pickup Enabled service parameter.

When this parameter is enabled, Cisco Unified Communications Manager automatically connects users to the incoming call in their own pickup group, in another pickup group, or a pickup group that is associated with their own group after users press the appropriate softkey on the phone. This action requires only one keystroke.
Auto call pickup connects the user to an incoming call in the group of the user. When the user presses the PickUp softkey on the phone, Cisco Unified Communications Manager locates the incoming call in the group and completes the call connection. If automation is not enabled, the user must press the softkeys, PickUp and Answer, to make the call connection.

Auto group call pickup connects the user to an incoming call in another pickup group. The user presses the GPickUp softkey on the phone, then dials the group number of another pickup group. Upon receiving the pickup group number, Cisco Unified Communications Manager completes the call connection. If auto group call pickup is not enabled, the user must press the GPickUp softkey, dial the group number of another pickup group, and answer the call to make the connection.

Auto other group pickup connects the user to an incoming call in a group that is associated with the group of the user. The user presses the OPickUp softkey on the phone. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups in the sequence that the administrator enters in the Call Pickup Group Configuration window and completes the call connection after the call is found. If automation is not enabled, the user must press the softkeys, OPickUp and Answer, to make the call connection.

Auto directed call pickup connects the user to an incoming call in a group that is associated with the group of the user. The user presses the GPickUp softkey on the phone, then dials the DN of the ringing phone. Upon receiving the DN, Cisco Unified Communications Manager completes the call connection. If auto directed call pickup is not enabled, the user must press the GPickUp softkey, dial the DN of the ringing phone, and answer the call that will now ring on the user phone to make the connection.

**Note**
CTI applications support monitoring the party whose call is picked up. CTI applications do not support monitoring the pickup requester or the destination of the call that is picked up. Hence, Cisco Unified Communications Manager Assistant does not support auto call pickup (one-touch call pickup).

**Note**
Auto call pickup interacts with Cisco Unified Mobility features on a limited basis. See “Auto Call Pickup” in the *Cisco Unified Communications Manager Features and Services Guide* for details.

### Call Pickup No Answer

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the call forward that is configured on the phone gets ignored when one of the pickup softkeys is pressed. If the call pickup requestor does not answer the call, the original call gets restored after the pickup no answer timer expires.

### Call Pickup Busy

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call gets restored while the call pickup requestor phone is busy.

### Call Pickup No Bandwidth

When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the original call gets restored when no bandwidth exists between the call originator and requestor phones.

**Additional Information**
See the “Related Topics” section on page 6-34.
Using Call Pickup Features with Hunt Lists

You can assign a call pickup group to a hunt pilot DN. Doing this affects how call pickup works. Users can pick up calls that are alerting in the line group members. If call pickup group notification is enabled, calls alerting in line group members get notified to the devices that are associated with the same call pickup group.

The service parameter “Allow Calls to be picked up from Line Group Members” controls this behavior. When this service parameter is set to False (the default), when line group members are included as part of a call pickup group, calls alerting in the line group members cannot be picked up from other call pickup group members. This is the same behavior as in Cisco Unified Communications Manager releases before this service parameter got added.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, any call pickup group configuration at the hunt pilot gets ignored. Alerting calls at the hunt list will neither get notified for pick up to the hunt pilot’s call pickup group, nor will those calls get picked up. When the service parameter “Allow Calls to be picked up from Line Group Members” is set to False, any call pickup group configuration at the line group members gets ignored.

Figure 6-9 and Figure 6-10 provide examples of the effects of this configuration.

Figure 6-9 Using Call Pickup Features with Hunt Lists Example 1
In Figure 6-9, when the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at Phone 3002 or Phone 3003 cannot get picked up even though Hunt Pilot (2000) is in Pickup Group 1. If the service parameter is set to False, calls alerting at 3001, 3002, 3003 or 3004 can get picked up from members associated with Pickup Group 1.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, if both hunt pilot and line group members are included in a call pickup group, only line group members’ call pickup group will be notified of calls available for pick up. Also calls alerting in the line group members can be picked up by lines associated with the same call pickup group as the line group members.

In Figure 6-10, when the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at Phone 3001 or Phone 3002 get notified to all of the members associated with Pickup Group 1: 3001, 3002 and 4001. If the service parameter is set to False, calls alerting at 3001, 3002, 3003 or 3004 get notified to 3003, 3004 and 4002.

When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, calls alerting at the line group members will be notified for pickup. But the pickup notification timer gets reset every time the call moves from one member to another. This results in multiple pickup notifications (to corresponding pickup group members) for the same call as it moves from one line group member to another. This notification gets provided if the “old” and “new” alerting line group member is in the same or different call pickup group. Call pickup notifications include the caller and the line group member information.
When the service parameter “Allow Calls to be picked up from Line Group Members” is set to True, the longest alerting call gets determined by the amount of time a call has been alerting in one specific call pickup group. If the call moves to another line group member that is in another call pickup group, the longest alerting timer gets reset. Also, if the call moves to another line group member that is not in any call pickup group, the longest alerting timer is reset.

Broadcast call distribution algorithm is not supported for calls to be picked up from line group members when the “Allow Calls to be picked up from Line Group Members” is enabled.

**Using Call Pickup Features with Partitions to Restrict Access**

You can restrict access to call pickup groups by assigning a partition to the call pickup group number. When this configuration is used, only the phones that have a calling search space that includes the partition with the call pickup group number can participate in that call pickup group. Make sure that the combination of partition and group number is unique throughout the system.

- If call pickup group numbers are assigned to a partition, only those phones that can dial numbers in that partition can use the call pickup group.

- If partitions represent tenants in a multitenant configuration, make sure that the pickup groups are assigned to the appropriate partition for each tenant.

A multitenant configuration provides an example of using partitions with call pickup groups. Assign the pickup groups to the appropriate partition for each tenant, and the group number will not be visible to other tenants.

With the Directed Call Pickup feature, the calling search space of the user who requests the Directed Call Pickup feature must contain the partition of the DN from which the user wants to pick up a call.

**Additional Information**

See the “Related Topics” section on page 6-34.

**Call Pickup Notification**

The Call Pickup Notification feature provides an audio or visual, or both, notification on Cisco Unified IP Phones when other members of a pickup group receive a call. Call Pickup Notification gets configured in three configuration windows for three types of settings: system, call pickup group, DN/phone.

- **Service Parameters Configuration**—The type of audio notification (beep or ring) to be heard when a phone is idle or busy gets set from the Service Parameters Configuration window. This setting becomes the system default.

- **Call Pickup Group Configuration**—The type of notification for each call pickup group gets configured from the Call Pickup Group Configuration window in Cisco Unified Communications Manager Administration. In addition to configuring the type of notification, you can configure the time, in seconds, to delay the audio and visual alerts after the call comes into that group. This allows the original called party a chance to pick up the call prior to the audio and/or visual alert being sent to the pickup group. See the “Call Pickup Group Configuration Settings” section on page 6-29.

  - To configure whether the notification will be audio or visual, or both, use the configuration settings in the Call Pickup Group Notification Settings section of the Call Pickup Group Configuration window. The notification gets sent only to the primary line of a device.
To configure the visual notification on the Call Pickup Group Configuration window, use the configuration settings in the Call Information Display For Call Pickup Group Notification section. This setting allows the administrator to have detailed calling party and/or called party information in the notification message. The display will contain the name of calling/called party if available. If not, the number will display. The visual notification comprises a message on the phone status line.

- Directory Number Configuration—This window provides fields where you can configure the audio alert setting for each phone. Configure the type of audio alert for phones by using the Pickup Audio Alert Setting. This lets users configure the type of audio alert to be provided when phone is idle or has an active call. See “Directory Number Configuration Settings” in the Cisco Unified Communications Manager Administration Guide.

Additional Information
See the “Related Topics” section on page 6-34.

System Requirements for Call Pickup

To operate, call pickup requires the following software and hardware components:

- Cisco Unified Communications Manager
- Table 6-5 lists the supported Cisco Unified IP Phones

Table 6-5 Cisco Unified IP Phones That Support Call Pickup

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Call Pickup Feature</th>
<th>Softkey</th>
<th>Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6900 Series (except 6901)</td>
<td>Call Pickup</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Group Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directed Call Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone 6911</td>
<td>does not support softkeys; the system administrator configures a feature number for Call Pickup, and the user presses the feature key and then dials the call pickup feature number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7900 Series</td>
<td>Call Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Group Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directed Call Pickup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See the “Related Topics” section on page 6-34.
Table 6-5  Cisco Unified IP Phones That Support Call Pickup (continued)

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Call Pickup Feature</th>
<th>Softkey</th>
<th>Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 8900 Series</td>
<td>Call Pickup</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Group Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directed Call Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified IP Phone 9900 Series</td>
<td>Call Pickup</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Group Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directed Call Pickup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information about Cisco Unified IP Phones and Call Pickup, see the phone user guides at the following URLs:


*Note*  The administrator must add the Other Pickup (OPickUp) softkey to the softkey templates. Configure Call Pickup, Group Call Pickup, Other Pickup, and Directed Call Pickup on the phone button template by using the programmable line key feature (see “Programmable Line Keys” in the *Cisco Unified Communications Manager System Guide*).

**Additional Information**

See the “Related Topics” section on page 6-34.

**Interactions and Restrictions**

The following sections describe the interactions and restrictions for call pickup:

- Interactions, page 6-24
- Restrictions, page 6-25

**Additional Information**

See the “Related Topics” section on page 6-34.
Interactions

The following sections describe how call pickup interacts with Cisco Unified Communications Manager applications and call processing:

- Route Plan Report, page 6-24
- Calling Search Space and Partitions, page 6-24
- Time of Day, page 6-24
- Call Accounting, page 6-24
- Dependency Records, page 6-25

Route Plan Report

The route plan report displays the patterns and DNs that are configured in Cisco Unified Communications Manager. Use the route plan report to look for overlapping patterns and DNs before assigning a DN to call pickup group. See the Route Plan Report chapter in the Cisco Unified Communications Manager Administration Guide.

Calling Search Space and Partitions

Assign a partition to the Call Pickup Group number to limit call pickup access to users on the basis of the device calling search space. See “Calling Search Space Configuration” and “Partition Configuration” in the Cisco Unified Communications Manager Administration Guide.

Time of Day

To pick up calls from a group that is associated with your own group, you must configure the calling search space, partition, and the Time of Day (TOD) parameter for members in the associated group to be active and able to accept calls within the same time period as your own group. TOD associates a time stamp to the calling search space and partition.

For example, a partition, ABC, remains active between 9 am to 5 pm. A calling search space, cssABC, contains partition ABC. A pickup group, pickABC contains phone 1 and phone 2. Phone 1 and phone 2 reside in the same calling search space, cssABC. If phone 1 rings at 5:30 pm and phone 2 tries to pick up the call, this attempt fails because the partition is not active after 5 pm. If phone 1 rings at 9:30 am, phone 2 can pick up the call.

Call Accounting

Call pickup features interact with call accounting.

- When a call pickup occurs via auto call pickup, the system generates two call detail records (CDRs). One CDR applies to the original call that is cleared, and another CDR applies to the requesting call that is connected.
- When a call pickup occurs via non-auto call pickup, the system generates one call detail record, which applies to the requesting call that is connected.
- A CDR search returns all CDRs that match a specific time range and other search criteria as specified. If users are interested in the type of call that is associated with a particular CDR, the search result displays a call type field that indicates whether the call is a pickup call.
Dependency Records

If you need to find devices to which a specific call pickup number is assigned, click the Dependency Records link that the Cisco Unified Communications Manager Administration Call Pickup Group Configuration window provides. The Dependency Records Summary window displays information about devices that are using the call pickup number.

If a pickup group is associated with other pickup groups, the dependency record of the pickup group shows the association information. For example, if pickup group A is associated with pickup group B and pickup group C, the dependency record of pickup group A shows the information on the association of pickup group A to pickup groups B and C.

To find out more information about the devices, click the device, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

For more information about Dependency Records, see “Accessing Dependency Records” in the Cisco Unified Communications Manager Administration Guide.

Additional Information
See the “Related Topics” section on page 6-34.

Restrictions

The following restrictions apply to call pickup group:

- Although different lines on a phone can be assigned to different call pickup groups, Cisco does not recommend this setup because it can be confusing to users.
- You cannot delete a call pickup group number when it is assigned to a line or DN. To determine which lines are using the call pickup group number, use Dependency Records. To delete a call pickup group number, reassign a new call pickup group number to each line or DN.
- When you update a call pickup group number, Cisco Unified Communications Manager automatically updates all directory numbers that are assigned to that call pickup group.
- The system does not support call pickup notification, audio, and visual alert on Cisco Unified IP Phones 7940 and 7960 that are running SIP.
- Call pickup notification, audio, and visual alert only supports licensed, third-party phones that are running SIP.
- Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.
- If a device belongs to a hunt list and the device rings due to a call that was made by calling the hunt pilot number, users cannot use the Directed Call Pickup feature to pick up such a call.

Additional Information
See the “Related Topics” section on page 6-34.

Installing and Activating Call Pickup

Call pickup, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.
Additional Information

See the “Related Topics” section on page 6-34.

Configuring Call Pickup Features

This section contains the following information:

- Setting the Service Parameters for Call Pickup, page 6-26

Tip

Before you configure call pickup, review the “Configuration Checklist for Call Pickup and Group Call Pickup” section on page 6-1, the “Configuration Checklist for Other Group Pickup” section on page 6-3, the “Configuration Checklist for Directed Call Pickup” section on page 6-5, and the “Configuration Checklist for BLF Call Pickup” section on page 6-7.

Setting the Service Parameters for Call Pickup

Cisco Unified Communications Manager provides the following clusterwide service parameters for call pickup features. Each service parameter includes a default and requires no special configuration.

- Auto Call Pickup Enabled—Default specifies False. This parameter determines whether the auto call pickup feature is enabled. To enable this capability, set the field to True.

- Call Pickup Locating Timer—Default specifies 1 second. This service parameter specifies the maximum time, in seconds, for a pickup to wait to get all alerting calls in the pickup groups from all of the nodes in the cluster.

- Call Pickup No Answer Timer—Default specifies 12 seconds. This required parameter specifies the maximum time, in seconds, to wait before restoring the original call if a user, who initiates a pickup request, decides not to pick up the call.

Note

To set the timers, choose System > Service Parameters, choose the Advanced icon or click the Advanced button, and update the fields in the Clusterwide Parameters (Feature-Call Pickup) pane.

- Allow Calls to be picked up from Line Group Members—Default specifies False. When this parameter is set to True, any call pickup group configuration at the hunt pilot gets ignored. Alerting calls at the hunt list will neither get notified for pick up to hunt pilot's call pickup group, nor will those calls get picked up. When this parameter is set to False, any call pickup group configuration at the line group members gets ignored. For more information about the effect of this service parameter, see the “Using Call Pickup Features with Hunt Lists” section on page 6-19.

Additional Information

See the “Related Topics” section on page 6-34.
Configuring Call Pickup Groups

This section contains the following information:

- Configuring Call Pickup Groups, page 6-27
- Configuring a Call Pickup Group, page 6-28
- Call Pickup Group Configuration Settings, page 6-29
- Deleting a Call Pickup Group, page 6-32
- Defining a Pickup Group for Other Group Pickup, page 6-33
- Assigning a Call Pickup Group to Directory Numbers, page 6-33

Tip
Before you configure call pickup, review the “Configuration Checklist for Call Pickup and Group Call Pickup” section on page 6-1, the “Configuration Checklist for Other Group Pickup” section on page 6-3, the “Configuration Checklist for Directed Call Pickup” section on page 6-5, and the “Configuration Checklist for BLF Call Pickup” section on page 6-7.

Finding a Call Pickup Group

The Find and List window for call pickup group allows you to search for call pickup groups that you have configured in Cisco Unified Communications Manager Administration.

Because you may have several call pickup groups in your network, Cisco Unified Communications Manager lets you locate call pickup groups on the basis of specific criteria. Use the following procedure to locate call pickup groups.

Note
During your work in a browser session, Cisco Unified Communications Manager Administration retains your call pickup group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your call pickup group search preferences until you modify your search or close the browser.

Procedure

Step 1
Choose Call Routing > Call Pickup Group.

The Find and List Call Pickup Groups window displays.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records,

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.
Note: To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the Clear Filter button to remove all added search criteria.

Step 3 Click Find.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note: You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note: To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information

See the “Related Topics” section on page 6-34.

Configuring a Call Pickup Group

This section describes how to add, copy, and update a single call pickup group.

Procedure

Step 1 Choose Call Routing > Call Pickup Group.

Step 2 Perform one of the following tasks:

- To add a new Call Pickup Group, click Add New.
- To copy a Call Pickup Group, use the procedure in the “Configuring Call Pickup Groups” section on page 6-27 to locate the call pickup group. Click the Copy icon.
- To update a Call Pickup Group, use the procedure in the “Configuring Call Pickup Groups” section on page 6-27 to locate the call pickup group.

The Call Pickup Group Configuration window displays.

Step 3 Enter or update the appropriate settings as described in Table 6-6.

Step 4 To save the new or changed call pickup groups in the database, click Save.
Call Pickup Group Configuration Settings

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a Cisco Unified IP Phone. Use the softkey, PickUp, for this type of call pickup.

The Group Call Pickup feature allows users to pick up incoming calls in another group. User must dial the appropriate call pickup group number when this feature is activated from a Cisco Unified IP Phone. Use the softkey, GPickUp, for this type of call pickup.

The same procedures apply for configuring call pickup and group call pickup features. Group call pickup numbers apply to lines or directory numbers.

Table 6-1 provides a checklist to configure Call Pickup and Group Call Pickup features. For more information on these features, see the “Introducing Call Pickup” section on page 6-10 and the “Related Topics” section on page 6-34.

Table 6-6 describes the call pickup group configuration settings.

### Table 6-6 Call Pickup Group Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Pickup Group Name</td>
<td>Enter up to 100 alphanumeric characters. For example, Operations.</td>
</tr>
<tr>
<td></td>
<td>The pickup group name associates with the pickup group number.</td>
</tr>
<tr>
<td></td>
<td>You can choose a pickup group by the pickup group name.</td>
</tr>
<tr>
<td>Call Pickup Group Number</td>
<td>Enter a unique directory number (integers) for the call pickup group that you want to add.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 24 digits. The following characters are allowed: numeric (0 to 9), A through D, plus (+), pound (#), and asterisk (*). If a number begins with the international escape character (+), you must precede the + with a backslash ().</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the call pickup group (for example, Operations Department Group Pickup).</td>
</tr>
</tbody>
</table>
Chapter 6      Call Pickup

Configuring Call Pickup Groups

Partition If you want to use a partition to restrict access to the call pickup group, choose the desired partition from the drop-down list box. If you do not want to restrict access to the call pickup group, choose <None> for the partition.

You can configure the number of partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Find and List Partitions window. See the “Searching for a Partition” section in the *Cisco Unified Communications Manager Administration Guide*.

**Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose **CCMAdmin Parameters**.

**Note** Make sure that the combination of call pickup group number and partition is unique within the Cisco Unified Communications Manager cluster.

### Call Pickup Group Notification Settings

<table>
<thead>
<tr>
<th>Call Pickup Group Notification Policy</th>
<th>From the drop-down list box, choose one of the following notification types:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• No Alert</td>
</tr>
<tr>
<td></td>
<td>• Audio Alert</td>
</tr>
<tr>
<td></td>
<td>• Visual Alert</td>
</tr>
<tr>
<td></td>
<td>• Audio and Visual Alert</td>
</tr>
</tbody>
</table>

| Call Pickup Group Notification Timer (seconds) | Enter the seconds of delay (integer in the range of 1 to 300) between the time that the call first comes into the original called party and the time that the notification to the rest of the call pickup group is to occur. |
Table 6-6  Call Pickup Group Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Information Display For Call Pickup Group Notification</td>
<td></td>
</tr>
<tr>
<td>Calling Party Information</td>
<td>Check the check box if you want the visual notification message to the call pickup group to include identification of the calling party. The system only makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert. If you choose to display both Calling Party Information and Called Party Information, only the first 11 characters of each display. If you choose to display only one or the other, the first 23 characters display. However, when the display name contains a feature tag without an associated number (such as Conference -&gt; Alice), the system does not limit the number of characters in this way. <strong>Note</strong> In the case of multiple active notification alerts, the latest visual alert overwrites the previous ones. When a user activates call pickup, the user connects to the earliest call that is available for pickup, even if that visual alert does currently display on the phone. You can avoid this mismatch by using visual notification without displaying calling or called party information. With this configuration, a generic message reading, “Call(s) available for Pickup” displays. The user can obtain the caller identification if Auto Call Pickup (AutoCallPickupEnabled service parameter) is disabled; see the “Auto Call Pickup” section on page 6-17 for more information.</td>
</tr>
<tr>
<td>Called Party Information</td>
<td>Check the check box if you want the visual notification message to the call pickup group to include identification of the original called party. The system makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert. If you choose to display both Calling Party Information and Called Party Information, only the first 11 characters of each display. If you choose to display only one or the other, the first 23 characters display. However, when the display name contains a feature tag without an associated number (such as Conference -&gt; Alice), the system does not limit the number of characters in this way. <strong>Note</strong> In the case of multiple active notification alerts, the latest visual alert overwrites the previous ones. However, when a user activates call pickup, the user connects to the earliest that is call available for pickup, even if that visual alert does not currently display on the phone. You can avoid this mismatch by using visual notification without displaying calling or called party information. With this configuration, a generic message reading, “Call(s) available for Pickup” displays. The user can obtain the caller identification if Auto Call Pickup (AutoCallPickupEnabled service parameter) is disabled; see the “Auto Call Pickup” section on page 6-17 for more information.</td>
</tr>
</tbody>
</table>
Table 6-6  Call Pickup Group Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Call Pickup Group Information—Find Pickup Numbers by Numbers/Partition</td>
<td></td>
</tr>
<tr>
<td>Partition</td>
<td>See Partition in Call Pickup Group Information in this table.</td>
</tr>
<tr>
<td>Call Pickup Group Numbers Contain</td>
<td>Enter the DN or part of the DN of the call pickup group that you want to find; then, click <strong>Find</strong>.</td>
</tr>
<tr>
<td>Available Call Pickup Groups</td>
<td>To add a member to the associated call pickup group list in the Current Associated Call Pickup Groups area, choose a DN/partition from this list; then, click <strong>Add to Associated Pickup Groups</strong>. The group that is being configured automatically gets added to the list of Current Associated Call Pickup Groups. This allows pickup of calls within your own group by using the OPickUp softkey.</td>
</tr>
<tr>
<td>Associated Call Pickup Group Information—Current Associated Call Pickup Groups</td>
<td></td>
</tr>
<tr>
<td>Selected Call Pickup Groups</td>
<td>To change order of the Call Pickup Groups listings, use the Up and Down arrows on the right side of this box to move the listings. Click <strong>Reverse Order of Selected Numbers</strong> to reverse the order of the listings. Use the Up and Down arrows below this box to move a call pickup group from this box to the Removed Call Pickup Groups box.</td>
</tr>
<tr>
<td>Removed Call Pickup Groups</td>
<td>Use the Up and Down arrows above this box to move a call pickup group from this box to the Selected Call Pickup Groups box.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 6-34.

Deleting a Call Pickup Group

This section describes how to delete a call pickup group from the Cisco Unified Communications Manager database.

Before You Begin

You cannot delete a call pickup group number that is assigned to a line or directory number. To see a list of the directory numbers that are using this call pickup group, click the **Dependency Records** link. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about Dependency Records, see the “Accessing Dependency Records” section in the Cisco Unified Communications Manager Administration Guide. To enable call pickup again for those directory numbers, you must reassign each of them to a new call pickup group. For details, see the “Assigning a Call Pickup Group to Directory Numbers” section on page 6-33.

Procedure

Step 1  Locate the call pickup group by using the procedure in the “Configuring Call Pickup Groups” section on page 6-27.

Step 2  Click the call pickup group that you want to delete.
Step 3 Click Delete.

The call pickup group no longer displays in the Find and List Call Pickup Groups window.

Additional Information
See the “Related Topics” section on page 6-34.

Defining a Pickup Group for Other Group Pickup

This section describes how to associate a call pickup group to your group for answering incoming calls for this associated group. You can associate up to 10 call pickup groups with your group. The priority of answering calls for the associated groups goes from the first associated group to the last associated group on the associated group list. You can organize the list in the Call Pickup Group Configuration window as described in Table 6-1.

Procedure

Step 1 Locate your group by using the procedure in the “Configuring Call Pickup Groups” section on page 6-27.
Step 2 In the Call Pickup Group Configuration window, scroll down to the Associated Call Pickup Group Information area.
Step 3 Enter information in the appropriate fields as described in Table 6-6.
Step 4 Click Save.

Additional Information
See the “Related Topics” section on page 6-34.

Assigning a Call Pickup Group to Directory Numbers

This section describes how to assign a call pickup group to a directory number. Only directory numbers that are assigned to a call pickup group can use call pickup, group call pickup, BLF call pickup, other group pickup, and directed call pickup.

Before You Begin
Before you can assign a call pickup group to a directory number, you must create the call pickup group as described in the “Configuring a Call Pickup Group” section on page 6-28.

Procedure

Step 1 Choose Device > Phone or Call Routing > Directory Number.
Step 2 Enter the appropriate search criteria to find the phone or directory number that you want to assign to a call pickup group and click Find.

A list of phones or directory numbers that match the search criteria displays.
Step 3  Choose the phone or directory number to which you want to assign a call pickup group.

Step 4  If you are using the Directory Number Configuration window, proceed to Step 6.

Step 5  From the Association Information list on the Phone Configuration window, choose the directory number to which the call pickup group will be assigned.

Step 6  From the Call Pickup Group drop-down list box that displays in the Call Forward and Call Pickup Settings area, choose the desired call pickup group.

Step 7  To save the changes in the database, click Save.

Additional Information
See the “Related Topics” section on page 6-34.

Assigning a Call Pickup Group to Hunt Pilots

This section describes how to assign a call pickup group to a hunt pilot. Only hunt lists that are assigned to a call pickup group can use call pickup, group call pickup, BLF call pickup, other group pickup, and directed call pickup.

Before You Begin
Before you can assign a call pickup group to a hunt list, you must create the call pickup group as described in the “Configuring a Call Pickup Group” section on page 6-28.

Procedure

Step 1  Choose Call Routing > Route/Hunt > Hunt Pilot.

Step 2  Enter the appropriate search criteria to find the hunt pilot that you want to assign to a call pickup group and click Find. A list of hunt pilots that match the search criteria displays.

Step 3  Choose the hunt pilot to which you want to assign a call pickup group.

Step 4  From the Call Pickup Group drop-down list box that displays in the Hunt Forward Settings area, choose the desired call pickup group.

Step 5  To save the changes in the database, click Save.

Additional Information
• Using Call Pickup Features with Hunt Lists, page 6-19
• Related Topics, page 6-34.

Related Topics
• Configuration Checklist for Call Pickup and Group Call Pickup, page 6-1
• Configuration Checklist for Other Group Pickup, page 6-3
• Configuration Checklist for Directed Call Pickup, page 6-5
• Configuration Checklist for BLF Call Pickup, page 6-7
• Introducing Call Pickup, page 6-10
• Call Pickup, page 6-11
• Group Call Pickup, page 6-11
• Other Group Pickup, page 6-12
• Directed Call Pickup, page 6-12
• Busy Lamp Field Call Pickup, page 6-16
• Auto Call Pickup, page 6-17
• Using Call Pickup Features with Partitions to Restrict Access, page 6-21
• Call Pickup Notification, page 6-21
• System Requirements for Call Pickup, page 6-22
• Interactions and Restrictions, page 6-23
• Installing and Activating Call Pickup, page 6-25
• Configuring Call Pickup Features, page 6-26
• Setting the Service Parameters for Call Pickup, page 6-26
• Configuring Call Pickup Groups, page 6-27
• Finding a Call Pickup Group, page 6-27
• Configuring a Call Pickup Group, page 6-28
• Call Pickup Group Configuration Settings, page 6-29
• Deleting a Call Pickup Group, page 6-32
• Defining a Pickup Group for Other Group Pickup, page 6-33
• Assigning a Call Pickup Group to Directory Numbers, page 6-33
• Directory Number Configuration, *Cisco Unified Communications Manager Administration Guide*
• *Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide*
• Partition Configuration, *Cisco Unified Communications Manager Administration Guide*
• Route Plan Report, *Cisco Unified Communications Manager Administration Guide*
• Time-of-Day Routing, *Cisco Unified Communications Manager System Guide*
• Softkey Template Configuration, *Cisco Unified Communications Manager Administration Guide*
• *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* (all models)
• Cisco Unified IP Phone user documentation and release notes (all models)
Call throttling allows Cisco Unified Communications Manager to automatically throttle (deny) new call attempts when it determines that various factors, such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation or other such events, could result in a potential delay to dial tone (the interval users experience from going off hook until they receive dial tone).

This chapter provides the following information about call throttling:

- Introducing Call Throttling, page 7-1
- Troubleshooting Call Throttling, page 7-2
- Related Topic, page 7-3

Introducing Call Throttling

Call throttling occurs automatically when Cisco Unified Communications Manager determines such conditions to be present, and the system exits throttling automatically when such conditions are alleviated. You can configure the parameters that are associated with entering and exiting call throttling through several service parameters in Cisco Unified Communications Manager Administration (System > Service Parameters) although Cisco does not advise modification of these parameters unless recommended by Cisco customer support. See Service Parameter Configuration in the Cisco Unified Communications Manager Administration Guide for information on accessing and configuring service parameters.

Cisco Unified Communications Manager uses the values that are specified in the call-throttling-related parameters to evaluate the possibility of a delay to dial tone and also to determine when conditions no longer necessitate call throttling. When throttling is necessary to prevent excessive delay to dial tone, Cisco Unified Communications Manager enters a Code Yellow state, and new call attempts are throttled (denied). You can disable call throttling via the System Throttle Sample Size service parameter, but Cisco does not recommend disabling call throttling. The following list defines several of the call throttling-related service parameters:

- Code Yellow Entry Latency defines the maximum allowable delay, in milliseconds, to handle SDL messages that are sent to Cisco Unified Communications Manager by the various devices in the system as well as the wealth of internal messages that are received and sent by Cisco Unified Communications Manager for various activities such as KeepAlives, change notification, and many more types of internal messaging. If the calculated average expected delay is more than the value that is specified in this service parameter, Cisco Unified Communications Manager enters a Code Yellow state to initiate call throttling, and stops accepting new calls.
Troubleshooting Call Throttling

- Code Yellow Exit Latency Calculation determines the acceptable percentage of Code Yellow Entry Latency to specify exit criteria for leaving the Code Yellow state (Code Yellow exit latency) when Cisco Unified Communications Manager has initiated call throttling. The basis for the value that you specify in this parameter comprises a formula that uses the value in the Code Yellow Entry Latency parameter, which specifies the delay in milliseconds. To arrive at a percentage, use the following formula: Code Yellow Entry Latency value multiplied by the Code Yellow Exit Latency value. For example:

  Code Yellow Entry Latency service parameter value: 20 msec
  Code Yellow Exit Latency service parameter value: 40%

  Code Yellow Exit Latency value = 20 X 0.4 = 8 msec, which means Cisco Unified Communications Manager exits Code Yellow state if the calculated message latency drops to 8 msec or lower.

  To get out of the Code Yellow state, Cisco Unified Communications Manager ensures that the average expected delay is less than the value of the Code Yellow exit latency.

- Code Yellow Duration specifies the number of minutes that a Cisco Unified Communications Manager system can remain in a Code Yellow state (call throttling). If this duration is met and the system is still in Code Yellow state, Cisco Unified Communications Manager enters a Code Red state, which indicates that Cisco Unified Communications Manager has remained in a Code Yellow state for an extended period and cannot recover. When Cisco Unified Communications Manager enters a Code Red state, the Cisco CallManager service restarts, which also produces a memory dump that may be helpful for analyzing the failure.

- System Throttle Sample Size indicates the size of the sample, in seconds, that is used to calculate the average expected delay for Cisco Unified Communications Manager to handle an SDL message. For example, a sample size of 10 means that Cisco Unified Communications Manager must calculate a non-zero latency value for 10 consecutive seconds before it will calculate the average expected delay and compare it to the value in the Code Yellow Entry Latency parameter. You can disable call throttling via this parameter.

When delay to dial tone is calculated to be over the threshold that is configured in the call-throttling-related service parameters, Cisco Unified Communications Manager begins rejecting new calls. When call throttling is engaged, a user who attempts a new call will receive reorder tone and, depending on the phone model, may also receive a prompt on the phone display. Call throttling effectively avoids the problem in which a user tries to place a new call, but the length of delay between going off-hook and receiving dial tone is excessive enough to cause a reaction in the user (such as complaining to the system administrator or questioning whether the system is down or the phone is broken, for example). Cisco Unified Communications Manager uses a complex algorithm to constantly monitor the system to anticipate when such latency could occur.

When the delay to dial tone is within the guidelines of the call-throttling-related service parameters, Cisco Unified Communications Manager ceases throttling calls by exiting the Code Yellow state and new calls events are again allowed.

Troubleshooting Call Throttling

CCM/SDI and SDL trace files record call throttling events and can provide useful information. Also, you generally will require performance monitoring data for debugging. The Cisco CallManager System Performance object (viewable in the Real Time Monitoring Tool) includes a counter called ThrottlingSampleActivity, which indicates whether Cisco Unified Communications Manager has calculated a non-zero value for latency and helps you understand how busy the system is. Frequent non-zero values in this counter could indicate a potential overload condition on the system. To try to circumvent the possibility of a Code Yellow event, consider the possible causes of a system overload,
such as heavy call activity, low CPU availability to Cisco Unified Communications Manager, routing loops, disk I/O limitations, disk fragmentation or other such events, and begin to investigate those possibilities.

Generally, repeated call throttling events require assistance from the Cisco Technical Assistance Center (TAC). TAC will likely request these trace files for closer examination.

Related Topic

- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without the need to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Tip

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

This chapter provides the following information about calling party normalization:

- Configuration Checklist for Calling Party Normalization, page 8-1
- Introducing Calling Party Normalization, page 8-4
  - Globalizing the Calling Party Number, page 8-5
  - Localizing the Calling Party Number, page 8-7
  - Mapping the Global Party Calling Number to Its Local Variant, page 8-9
- System Requirements, page 8-10
- Interactions and Restrictions, page 8-10
- Installing and Activating Calling Party Normalization, page 8-15
- Configuring Calling Party Normalization, page 8-15
- Providing Information to End Users, page 8-26
- Related Topics, page 8-27

Configuration Checklist for Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without needing to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.
Table 8-1 lists the tasks that you perform to globalize and localize the calling party number. For more information on calling party normalization, see the “Introducing Calling Party Normalization” section on page 8-4 and the “Related Topics” section on page 8-27.

### Configuration Checklist for Calling Party Normalization

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Review the interactions and restrictions for this feature.</td>
<td>Globalizing the Calling Party Number, page 8-5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>If you have not already done so, activate the Cisco CallManager service in Cisco Unified Serviceability.</td>
<td>Cisco Unified Serviceability Administration Guide</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Globalizing the Calling Party Number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>If you want to do so, configure the Calling Party Number Type.</td>
<td>Globalizing the Calling Party Number, page 8-5</td>
</tr>
<tr>
<td></td>
<td>Configuring the Calling Party Number Type, page 8-17</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>For incoming national, international, subscriber, and unknown calls via the PSTN, create the prefixes that you want to associate with these types of calls. You create prefixes for device types; for example, phones, MGCP gateways, H.323 gateways/trunk, SIP trunks, and so on.</td>
<td>Globalizing the Calling Party Number, page 8-5</td>
</tr>
<tr>
<td></td>
<td>Setting the Service Parameters for Calling Party Normalization, page 8-15</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the fields in Table 8-7 to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.</td>
<td>Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number, page 8-25</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Create various partitions for the calling party transformation patterns under Call Routing &gt; Class of Control &gt; Calling Search Space. Create different partitions and calling search spaces for different calling party transformation patterns and different number types, respectively.</td>
<td>Partition Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
### Table 8-1  Configuration Checklist for Calling Party Normalization (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> Create incoming calling party number calling search spaces (CSS) for the various calling party number types under Call Routing &gt; Class of Control &gt; Calling Search Space; for example, create a CSS for the national calling party number type, a CSS for the international calling party number type, and so on. In the Calling Search Space Configuration window for the CSS, move the partition that you created for the calling party transformation pattern to the Available Partitions pane. Perform this task for each CSS that you create.</td>
<td>Calling Search Space Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 6</strong> Choose <strong>Call Routing &gt; Transformation Patterns &gt; Calling Party Transformation Pattern</strong> to create the Calling Party Transformation Pattern; in the Calling Party Transformation Pattern Configuration window, assign the partition that you associated with the incoming calling party transformation CSS to the calling party transformation pattern.</td>
<td>Calling Party Transformation Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 7</strong> Choose the appropriate Incoming Calling Party Transformation CSS in the device configuration window; for example, in the Gateway Configuration, SIP Trunk Configuration, and so on. <strong>Tip</strong> To choose the incoming calling party number CSS in the device configuration window, configure the Calling Search Space settings for the calling party number types in the Incoming Calling Party Number Settings pane.</td>
<td>Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number, page 8-25</td>
</tr>
</tbody>
</table>

### Localizing the Calling Party Number

| **Step 1** | Create a partition for the calling party transformation pattern under Call Routing > Class of Control > Calling Search Space. | Partition Configuration Settings, Cisco Unified Communications Manager Administration Guide |
| **Step 2** | Create the Calling Party Transformation calling search space (CSS) under Call Routing > Class of Control > Calling Search Space; in the Calling Search Space Configuration window for the calling party transformation CSS, move the partition that you created for the calling party transformation pattern to the Available Partitions pane. | Calling Search Space Configuration Settings, Cisco Unified Communications Manager Administration Guide |
Introducing Calling Party Normalization

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without the need to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Tip

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

This section contains information on the following topics:

- Globalizing the Calling Party Number, page 8-5
- Localizing the Calling Party Number, page 8-7
- Mapping the Global Party Calling Number to Its Local Variant, page 8-9

---

### Table 8-1 Configuration Checklist for Calling Party Normalization (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Choose Call Routing &gt; Transformation Patterns &gt; Calling Party Transformation Pattern to create the Calling Party Transformation Pattern; in the Calling Party Transformation Pattern Configuration window, assign the partition that you associated with the calling party transformation CSS to the calling party transformation pattern.</td>
<td>Calling Party Transformation Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Choose the Calling Party Transformation CSS in the device configuration window; for example, in the Gateway Configuration, Phone Configuration, Trunk Configuration, and the CTI Route Point Configuration window. To choose the Calling Party Transformation CSS in the device configuration window, configure the Calling Party Transformation CSS setting (not the Calling Search Space setting). If you want the device to use the Calling Party Transformation CSS that is assigned to the device pool that the device uses, check the Use the Device Pool Calling Party Transformation CSS.</td>
<td>Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number, page 8-25</td>
</tr>
</tbody>
</table>
Globalizing the Calling Party Number

This section does not describe the international escape character, +, which you can configure for globalizing the calling party number. For information on the international escape character, see the “Using the International Escape Character +” in the Cisco Unified Communications Manager System Guide.

This section contains information on the following topics:

- Globalization of the Calling Party Number Description, page 8-5
- Configuration Windows in Cisco Unified Communications Manager Administration for Globalizing the Calling Party Number, page 8-6

Globalization of the Calling Party Number Description

To globalize the calling party number for calls that get routed to multiple geographical locations, Cisco Unified Communications Manager allows you to configure prefixes for required access codes, escape codes, country codes, and so on, based on the calling party number type that the PSTN provides. The calling party number type that the PSTN provides determines whether the incoming call arrives from the PSTN as a national, international, subscriber, or unknown call. For example, if the call comes from a caller in Hamburg to an enterprise gateway in Hamburg, the call arrives to Cisco Unified Communications Manager with calling party number 69XXXXXXX with number type of Subscriber. However, if the call comes from a caller in Frankfurt to an enterprise gateway in Hamburg, the call arrives to Cisco Unified Communications Manager with caller party number 69XXXXXXX with number type of National.

Configuring the Calling Party Number Type setting and prefixes in Cisco Unified Communications Manager Administration allows Cisco Unified Communications Manager to reformat the calling party number from the PSTN-localized version to the globally dialable version by prefixing required access codes, international access codes, and so on, to the calling party number. You can configure the Calling Party Number Type setting for various patterns, for example, translation patterns, calling party transformation patterns, and route patterns, for both called and calling parties to ensure that Cisco Unified Communications Manager stamps the number type during various stages of incoming and outgoing calls. After Cisco Unified Communications Manager globalizes the calling party number, the call gets routed as expected to its destination.

Tip

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the digits to strip fields to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. For more information, see the “Considerations for Configuring the Strip Digits Field” section on page 8-19.

Depending on your configuration for globalizing and localizing the calling party number, the phone user may see a localized number, a globalized number with access codes and prefixes, and/or the international escape character, +, in the calling party number. For example, the phone can show the localized calling party number on the phone screen and the globalized number in the call log directories on the phone. For example, the phone may show both the globalized and localized calling party number in the Call Details.
Chapter 8  Calling Party Normalization

Introducing Calling Party Normalization

To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, map the global calling party number to its local variant to route calls to the correct gateway; you can use route patterns and called party transformation patterns to route the call correctly, as the “Mapping the Global Party Calling Number to Its Local Variant” section on page 8-9 describes.

Configuration Windows in Cisco Unified Communications Manager Administration for Globalizing the Calling Party Number

Table 8-2 lists the configuration windows in Cisco Unified Communications Manager Administration where you can configure prefixes, the number of leading digits that you want to strip from the calling party number before applying the prefix, and the incoming calling party transformation CSS for various calling party number types (subscriber, national, and so on).

<table>
<thead>
<tr>
<th>Configuration Window</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Pool</td>
<td>You can configure prefixes in the device pool, which support digital gateways or trunks. In addition, if your service provider prepends digits to the calling party number, you can configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number before applying the prefix. In this window, you can apply an incoming calling party transformation CSS for various calling party number types; for example, subscriber, unknown, and so on, depending on the device type. Configuring this CSS ensures that the device can globalize the calling party number based on the calling party number type.</td>
</tr>
<tr>
<td>Gateway</td>
<td>You can configure prefixes for H.323, MGCP (T1-PRI/BRI), and MGCP (E1-PRI/BRI) gateways.</td>
</tr>
</tbody>
</table>

If you have gateways in multiple geographical locations, configure the prefix settings for each gateway in the Gateway Configuration window. For example, if you have a gateway in RTP and an incoming call arrives with caller ID 555 1212, you want to prefix the caller ID with 919 to yield 9195551212. However, if the call routes to another gateway, for example, in Dallas, which uses area code 214, before reaching its final destination, you want 91214 to display for the prefix instead of 91919.

To globalize calling party numbers for incoming calls, you must configure the prefixes for gateways that handle incoming calls. In addition, if your service provider prepends digits to the calling party number, you can configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number before applying the prefix.

In this window, you can apply the incoming calling party transformation CSS for various calling party number types; for example, subscriber, unknown, and so on, depending on the device type. Configuring this CSS ensures that the device can globalize the calling party number based on the calling party number type.

If you want to do so, you can apply the calling party transformation CSS that you chose in the device pool and applied to the device.
Localizing the Calling Party Number

For the final presentation of the calling party number, Cisco Unified Communications Manager allows you to configure calling party transformation patterns for each calling party number type (National, International, Subscriber, and Unknown), so the number displays on the phone as the end user expects it to display; that is, you can configure the calling party transformation pattern to strip digits or add digits to the calling party number. To present the shortest recognizable number on the phone, you can strip unnecessary country codes, international access codes, and so on, depending on the locations of the caller and the called parties.
Introducing Calling Party Normalization

You configure calling party transformation patterns to provide context-sensitive modifications to a calling party, not for routing purposes.

Example 8-1 shows how you can configure transformation patterns to localize a globalized calling party number.

Example 8-1  Localizing the Calling Party Presentation

You can globalize the calling party number before localizing the number. To globalize the calling party number in Example 8-1 before localizing the number, the administrator can configure the incoming gateway in Hamburg with the following information: Number Type of Subscriber with +4940 prefix; Number Type of National with +49 prefix; Number Type of International with + prefix. After the administrator configures the gateway, he configures the transformation patterns in Table 8-3.

To globalize the calling party number before localizing the number, Cisco Unified Communications Manager applies the prefix and digits-to-strip configuration based on the calling party number type before applying the calling party transformation.

For example, a call occurs between two parties in Hamburg. The incoming call over the PSTN in Hamburg gets globalized as +49 40 69XXXXXXX, but the administrator has configured multiple transformation patterns to localize the calling party number before it reaches the desktop phone of the called party in Hamburg. These transformation patterns, which use closest match routing to strip unnecessary digits, contain the configuration, as shown in Table 8-3:

<table>
<thead>
<tr>
<th>Pattern 1</th>
<th>Pattern 2</th>
<th>Pattern 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>+4940.(! (Pattern Setting)</td>
<td>+49.(!</td>
<td>+!.(!</td>
</tr>
<tr>
<td>discard Predot (Discard Digits Instructions Setting)</td>
<td>discard Predot</td>
<td>discard Predot</td>
</tr>
<tr>
<td>prefix 0 (Prefix Digits Setting)</td>
<td>prefix 00</td>
<td>prefix 000</td>
</tr>
<tr>
<td>Subscriber (Calling Party Number Type Setting)</td>
<td>National</td>
<td>International</td>
</tr>
</tbody>
</table>

By using digit analysis matching semantics, all the patterns in Table 8-3 match the provided dial string; however, Transformation Pattern 1, which constitutes the closest match for a call within Hamburg, indicates that if the call is from Germany and from Hamburg, strip the German country code, 49, and the Hamburg city code, 40, and add the prefix 0 to the calling party number. So, when both parties in a call are in Hamburg, +494069XXXXXX changes to 069XXXXXX.

If the caller is from Frankfurt, Transformation Pattern 1 does not match, but Transformation Patterns 2 and 3 match. Representing the best match, Transformation Pattern 2 indicates that the system needs to strip the + and the German country code, 49, and then prefix 00 to the calling party number. So, for a long-distance call from Frankfurt to Hamburg, +494069XXXXXXX changes to 0069XXXXXXX.

If the caller is international, Transformation Pattern 3 works because Cisco Unified Communications Manager strips the international escape character, +, and prefixes the German international code, 000, to the calling party number.
Tip

All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration localize the calling party number for themselves; to ensure that the device can localize the calling party number, you must configure the Calling Party Transformation CSS (calling search space) and assign this calling search space to the device. The Calling Party Transformation CSS takes on the attributes of the calling party transformation pattern, which you assign to the partition where the Calling Party Transformation CSS exists. If you want to do so, you can choose the Calling Party Transformation CSS in the device pool; when you assign the device pool to the device, the device uses the Calling Party Transformation CSS in the device pool; that is, if you check the Use Device Pool Calling Party Transformation CSS check box in the device configuration window.

The Calling Party Transformation CSS settings do not apply to T1-CAS and FXO ports on the gateway.

Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

**Mapping the Global Party Calling Number to Its Local Variant**

To ensure that the phone user does not need to edit the call log directory entry on the phone before placing a call, map the global calling party number to its local variant to route calls to the correct gateway; you can use route patterns and called party transformation patterns to route the call correctly, as Example 8-2 describes.

Example 8-2  **Mapping the Global Calling Party Number to Its Local Variant**

A Cisco Unified IP Phone in Hamburg (Phone Q) receives calls over the Hamburg or Frankfurt PSTN from different localized and globalized calling party numbers. To ensure that the phone user for the Phone Q does not need to edit the call log directory entry on the phone to return the call, you can associate the route patterns in Table 8-4 to the calling search space in the Phone Configuration window for Phone Q.

In Cisco Unified Communications Manager Administration, you configure the route patterns in Table 8-4 in the Route Patterns Configuration window (Call Routing > Route/Hunt > Route Patterns).

<table>
<thead>
<tr>
<th>Route Pattern</th>
<th>Configuration for Route Pattern Setting</th>
<th>Configuration for Discard Digits Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern 1</td>
<td>+4940.! Configured for local Hamburg callers that call by using a globalized calling party number.</td>
<td>discard Predot</td>
</tr>
<tr>
<td>Route Pattern 2</td>
<td>0.! Configured for local Hamburg callers that call by using a localized calling party number.</td>
<td>discard Predot</td>
</tr>
</tbody>
</table>
When Phone Q in Example 8-2 receives a call from the Hamburg calling party number, 69XXXXXXX, via the PSTN, the calling party number +49406XXXXXXX displays on the phone screen for Phone Q. If the phone user for Phone Q returns the call by using the globalized calling party number, Cisco Unified Communications Manager matches the pattern, +49.!, routes the call to the correct gateway, and sends the relevant digits. If the phone user for Phone Q returns the call by using the localized calling party number, Cisco Unified Communications Manager matches the pattern, 0.!, routes the call to the correct gateway, and sends the relevant digits.

When Phone Q in Example 8-2 gets a call from the Frankfurt calling party number XXXXXXX via the PSTN, the globalized calling party number +4969XXXXXXX displays on the phone screen for Phone Q, and the localized calling party number displays as 0069XXXXXXX. If the phone user for Phone Q returns the call by using the globalized calling party number, Cisco Unified Communications Manager matches the pattern, +49.!, routes the call to the correct gateway, and sends the relevant digits. If the phone user for Phone Q returns the call by using the localized calling party number, Cisco Unified Communications Manager matches the pattern, 0.0!, routes the call to the correct gateway, and sends the relevant digits.

System Requirements

The following system requirements apply to calling party normalization:
- Cisco Unified Communications Manager 7.1
- Cisco Unified IP Phones 7906, 7911, 7931, 7961, 7962, 7965, 7970, 7971, and 7975

Interactions and Restrictions

The following sections describe the interactions and restrictions for calling party normalization:
- Interactions, page 8-11
- Restrictions, page 8-14
Interactions

The following sections describe how calling party normalization interacts with Cisco Unified Communications Manager features and applications:

- Globalizing and Localizing Calling Party Numbers for Transferred Calls, page 8-11
- Globalizing and Localizing Calling Party Numbers for Forwarded Calls, page 8-11
- Bulk Administration Tool, page 8-12
- Call Detail Records, page 8-12
- Cisco Unified Communications Manager Assistant, page 8-12
- Cisco Unified Communications Manager CDR Analysis and Reporting, page 8-12
- Cisco Unity/Cisco Unity Connection, page 8-12
- Cisco Extension Mobility, page 8-13
- Device Mobility, page 8-13

Globalizing and Localizing Calling Party Numbers for Transferred Calls

The transfer feature relies on midcall updates, so depending on the scenario, a transferred call may not support globalization and localization of the calling party number. (Calling party normalization supports globalization and localization during call setup for each hop of the call, not for midcall updates.) For examples of how calling party normalization works for transferred calls, see the following sections:

- Calling Party Normalization for On Net Transferred Call Across a Gateway, page 8-11
- Calling Party Normalization for Transferred Call Through an Incoming Gateway, page 8-11

Calling Party Normalization for On Net Transferred Call Across a Gateway

Phone A with extension 12345 and phone number of 972 500 2345 calls Phone B with extension 54321 and phone number 972 500 4321; when the call arrives on extension 54321, calling party number 12345 displays on Phone B. Phone B transfers the call to Phone C in San Jose through a San Jose gateway. During the initiation of the transfer, Phone C displays the calling party number for Phone B as 972 500 4321. After the transfer completes, Phone C displays the calling party number for Phone A as 12345.

Calling Party Normalization for Transferred Call Through an Incoming Gateway

Via the PSTN in Dallas, a caller (Phone D) calls Phone E (Cisco Unified IP Phone), which uses extension 7891 and phone number 972 500 6789. On the incoming Dallas gateway, the caller information for Phone D displays as 500 1212/<Subscriber>. Phone E displays +1 972 500 1212 for the globalized calling party number and 500 1212 for the localized calling party number for Phone D. Phone E initiates a transfer to Phone C in San Jose across the San Jose gateway. During the initiation of the transfer, Phone C displays the calling party number for Phone E as 972 500 6789. After the transfer completes, Phone C displays the calling party number for Phone D as +1 972 500 1212.

Globalizing and Localizing Calling Party Numbers for Forwarded Calls

Forwarded calls support globalized and localized calling party numbers. Globalization and localization of the call occur during call setup for each hop of the call. Depending on the hop for the call and the configuration of the gateway, that is, the calling party transformation and prefix configuration on the
gateway, the globalized version or the localized version (or both) may display on the phone. See the following example, which describes how an incoming call via the PSTN gets forwarded to another geographic location.

For example, via the PSTN in Dallas, a caller with Phone F calls Phone G (Cisco Unified IP Phone), which has forwarded all calls to Phone H (Cisco Unified IP Phone) in San Jose. On the incoming Dallas gateway, the caller information for Phone F displays as 500 5555/Subscriber. On the outgoing gateway from Dallas to San Jose, the outgoing caller information for the Calling Party Transformation CSS comprises 972 500 5555/National. On the incoming gateway in San Jose, the calling party number gets prefixed with +1 for the National number type; on Phone H in San Jose, the localized calling party number for Phone F displays as 972 500 5555, and the globalized calling party number displays as +1 972 500 5555.

**Bulk Administration Tool**

For information on how calling party normalization relates to the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Call Detail Records**

For information on how calling party normalization impacts call detail records (CDRs), see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

**Cisco Unified Communications Manager Assistant**

Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring Cisco Unified Communications Manager Assistant, see the “Cisco Unified Communications Manager Assistant With Proxy Line Support” section on page 11-1 or the “Cisco Unified Communications Manager Assistant With Shared Line Support” section on page 12-1.

**Cisco Unified Communications Manager CDR Analysis and Reporting**

For information on how calling party normalization impacts Cisco Unified Communications Manager CDR Analysis and Reporting (CAR), see the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*.

**Cisco Unity/Cisco Unity Connection**

Cisco Unity and Cisco Unity Connection do not support the international escape character (+). Because these applications do not support the +, you must ensure that calls to Cisco Unity or Cisco Unity Connection do not contain the +, which ensures that voice-messaging features work as expected.

If you configure the + for the incoming prefix settings in Cisco Unified Communications Manager Administration to globalize the calling party number, the + gets inserted as a prefix to an incoming calling party number on a H.323, MGCP, or SIP gateway (or trunk, if applicable). If you configure calling party transformations, the device can localize the calling party number to transform the number to display differently than the globalized version. For example, a call from the North American
Numbering Plan arrives as a 10-digit calling party number, 2225551234. Cisco Unified Communications Manager prefixes +1 to the calling party number to display the E.164 formatted number as +12225551234. On a phone in North America, Cisco Unified Communications Manager uses a calling party transformation to convert +12225551234 to 10 digits before the number displays on the phone; on a phone outside of North America, Cisco Unified Communications Manager may transform the number to only strip the + and to prefix the 00, as in 0012225551234.

For Cisco Unity and Cisco Unity Connection to work as expected, treat these applications as devices and configure calling party transformations that ensure that the + does not get sent to these voice-messaging applications. If the Cisco Unity or Cisco Unity Connection server uses a North American-based dial plan, localize the calling party number to NANP format before the voice-mail application receives the calling party number. Because no calling party transformation options exist in Cisco Unified Communications Manager Administration for voice-messaging ports, make sure that you configure the calling party number transformations in the device pool that is associated with the voice-messaging ports. To localize the calling party number, also consider prefixing access codes, so the voice-messaging application easily can redial the number for certain features, such as Live Reply. For example, you can convert +12225551234 to 912225551234, and you can convert international number, +4423453456, to include the international escape code, 90114423453456.

Cisco Extension Mobility

Cisco Extension Mobility works as expected; that is, a phone user that is logged in to a Cisco Extension Mobility phone may see globalized or localized calling party numbers on the phone screen or in the call log directories on the phone.

Device Mobility

The following example shows how calling party normalization works when you move a phone from its home location, as supported with the device mobility feature in Cisco Unified Communications Manager.

A Cisco Unified IP Phone (Phone N) with home location in Dallas moves to San Jose. The Cisco Unified IP Phone in Dallas uses device pool, DP_Dallas, which has the Calling Party Transformation CSS as CallingTransform_Dallas; the CallingTransform_Dallas CSS contains the DallasPhone and the CommonTransform partitions. The roaming device in San Jose uses device pool, DP_SanJose, which has the Calling Party Transformation CSS as CallingTransform_SJ; the CallingTransform_SJ CSS contains the SJPhone and the CommonTransform partitions. Cisco Unified Communications Manager Administration contains the configuration in Table 8-5:

<table>
<thead>
<tr>
<th>Table 8-5</th>
<th>Globalizing and Localizing Calling Party Numbers with Device Mobility (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Calling Party Transformation Pattern 1</strong></td>
<td><strong>Calling Party Transformation Pattern 2</strong></td>
</tr>
<tr>
<td>- Pattern—+.@</td>
<td>- Pattern—+1.408!</td>
</tr>
<tr>
<td>- Partition—CommonTransform</td>
<td>- Partition—SJPhone</td>
</tr>
<tr>
<td>- Disregard Digits Instructions—Predot</td>
<td>- Discard Digits Instructions—Predot</td>
</tr>
<tr>
<td>- Calling Party Number Type—National</td>
<td>- Prefix—9</td>
</tr>
<tr>
<td>- Calling Party Number Type—Subscriber</td>
<td>- Calling Party Number Type—Subscriber</td>
</tr>
</tbody>
</table>
When the phone is in its home location in Dallas, a call comes via the PSTN from 408 500 1212 <National> in San Jose. On the incoming Dallas gateway, the calling party number gets converted to the global format of +1 408 500 1212. On the phone that currently is in Dallas, the calling party number displays as 1 408 500 1212.

When the phone is in its home location in Dallas, a call comes via the PSTN from 400 2323 <Subscriber> from a seven-digit dialing area in Dallas. On the incoming Dallas gateway, the calling party number gets converted to the global format of +1 972 400 2323. On the phone that currently is in Dallas, the calling party number displays as 9 400 2323.

When the phone is roaming in San Jose, a call comes via the PSTN from 972 500 1212 <National> in Dallas. On the incoming San Jose gateway, the calling party number gets converted to the global format of +1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 1 972 500 1212.

When the phone is roaming in San Jose, a call comes via the PSTN from 500 1212 <Subscriber> from a seven-digit dialing area in San Jose. On the incoming San Jose gateway, the calling party number gets converted to the global format of +1 408 500 1212. On the phone that currently is in San Jose, the calling party number displays as 9 500 1212.

Note

The Calling Party Transformation CSS of the roaming device pool overrides the device level configuration of the phone roaming within same DMG, even when the Use Device Pool Calling Party Transformation CSS check box in the phone configuration window remains unchecked.

Restrictions

Before you configure calling party normalization, review the following restrictions:

- The calling party number that displays for a shared line depends on the sequence of call control events in Cisco Unified Communications Manager. To avoid displaying an incorrect localized calling party number on a shared line, especially when the shared line occurs in different geographical locations, make sure that you configure the same Calling Party Transformation CSS for different devices that share the same line.

- SIP trunks and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway.

- SIP does not support the number type, so calls through SIP trunks only support the Incoming Number settings for calling party number types of Unknown.

- A QSIG configuration usually supports a uniform dial plan. Transformation of numbers and prefixes may cause feature interaction issues if you use QSIG.

- For localizing the calling party number, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

- The Calling Party Transformation CSS settings do not apply to T1-CAS and FXO ports on the gateway.
Cisco Unity and Cisco Unity Connection do not support the international escape character (+). Because these applications do not support the +, you must ensure that calls to Cisco Unity or Cisco Unity Connection do not contain the +, which ensures that voice-messaging features work as expected. For more information, see the “Cisco Unity/Cisco Unity Connection” section on page 8-12.

Installing and Activating Calling Party Normalization

After you install Cisco Unified Communications Manager, you can configure calling party normalization. Calling party normalization service parameters support the Cisco CallManager service, so activate the Cisco CallManager service in Cisco Unified Serviceability before you configure calling party normalization.

Configuring Calling Party Normalization

This section contains information on the following topics:

- Setting the Service Parameters for Calling Party Normalization, page 8-15
- Configuring the Calling Party Number Type, page 8-17
- Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows, page 8-18
- Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number, page 8-25

Tip

Before you configure calling party normalization, review the “Configuration Checklist for Calling Party Normalization” section on page 8-1.

Setting the Service Parameters for Calling Party Normalization

Tip

To locate the service parameters in Cisco Unified Communications Manager Administration, choose System > Service Parameters; choose the server and the Cisco CallManager service. After the parameters display, click Advanced. For information on the service parameter, click the hyperlink for the service parameter name or the question mark that displays in the upper, right corner of the window.

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can enter a colon (:) followed by the number of digits that you want to strip in the Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and/or Incoming Calling Party Subscriber Number Prefix service parameters to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. The value that you configure before the colon (:)

Tip

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can enter a colon (:) followed by the number of digits that you want to strip in the Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and/or Incoming Calling Party Subscriber Number Prefix service parameters to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. The value that you configure before the colon (:)
Chapter 8      Calling Party Normalization

represents the prefix; the value that you configure after the colon (:) specifies the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number before it applies the prefix.

For example, you configure +:1 in the incoming prefix service parameters, which alerts Cisco Unified Communications Manager to strip the first digit from the calling party number and then apply the international escape character +. If an incoming call arrives as 04423452345, Cisco Unified Communications Manager strips the first digit, in this case, zero, from the calling party number and prefixes the international escape character + to the calling party number. As a result, the calling party number gets transformed to +4423452345.

To strip digits without prefixing anything, you can configure the colon (:) in the incoming prefix service parameters without configuring a prefix. If you do not enter a prefix before the colon (:), Cisco Unified Communications Manager strips the number of leading digits that you specify and does not apply a prefix to the calling party number. For example, if you configure :2, Cisco Unified Communications Manager strips 2 leading digits without applying a prefix.

If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix. For example, if you enter +1:6 in the incoming prefix fields, and the calling party number contains 6 or fewer digits, Cisco Unified Communications Manager strips all digits and applies the prefix +1.

If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).

If you do not configure a colon (:) in the incoming prefix service parameters, Cisco Unified Communications Manager does not strip any digits from the calling party number; that is, unless you configure the incoming fields that are described Table 8-7, which support the configuration at the device level.

If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix.

Cisco Unified Communications Manager can strip up to 24 digits from the calling party number. If you enter :26 in the incoming prefix service parameters, Cisco Unified Communications Manager Administration displays a message and does not allow the configuration.

If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Tip

If you configure the incoming fields that display in the device configuration windows and the service parameters, Cisco Unified Communications Manager uses the configuration that you configured in the device configuration window.

Clusterwide Parameters (Device - PRI and MGCP Gateway)

- Incoming Calling Party National Number Prefix - MGCP
- Incoming Calling Party International Number Prefix - MGCP
- Incoming Calling Party Subscriber Number Prefix - MGCP
- Incoming Calling Party Unknown Number Prefix - MGCP
If you have a single H.323, MGCP (T1-PRI/BRI), or MGCP (E1-PRI/BRI) gateway in your network, you can configure the prefix service parameters, which support the Cisco CallManager service, for the particular gateway type in the Service Parameter Configuration window. If you configure the prefix service parameters for a particular gateway type, for example, H.323, be aware that all H.323 gateways that you configure in Cisco Unified Communications Manager Administration use the configuration from the service parameter unless you configure the prefix settings for a particular gateway in the Gateway Configuration window.

**Clusterwide Parameters (Device - H323)**

- Incoming Calling Party National Number Prefix - H.323
- Incoming Calling Party International Number Prefix - H.323
- Incoming Calling Party Subscriber Number Prefix - H.323
- Incoming Calling Party Unknown Number Prefix - H.323

**Tip**

If the incoming prefix service parameters for H.323 use the same prefix as the incoming prefix service parameters for the phone, the prefix gets used twice for the calling party: first, when the incoming call gets to the gateway and again, when the call terminates at the phone.

**Clusterwide Parameters (Device - SIP)**

Incoming Calling Party Unknown Number Prefix - SIP

**Configuring the Calling Party Number Type**

Configuring the Calling Party Number Type setting and prefixes in Cisco Unified Communications Manager Administration allows Cisco Unified Communications Manager to reformat the calling party number from the PSTN-localized version to the globally dialable version by prefixing required access codes, international access codes, and so on, to the calling party number. You can configure the Calling Party Number Type setting for various patterns for both called and calling parties to ensure that Cisco Unified Communications Manager stamps the number type during various stages of incoming and outgoing calls.

You configure the Calling Party Number Type setting in the Calling Party Transformation Pattern Configuration, Route Pattern Configuration, Hunt Pilot Configuration, Translation Pattern Configuration, and the Route List Detail Configuration windows in Cisco Unified Communications Manager Administration.

- **Route Pattern Configuration**, *Cisco Unified Communications Manager Administration Guide*
- **Hunt Pilot Configuration**, *Cisco Unified Communications Manager Administration Guide*
- **Calling Party Transformation Pattern Configuration Settings**, *Cisco Unified Communications Manager Administration Guide*
Table 8-6 describes the Calling Party Number Type setting that displays in Cisco Unified Communications Manager Administration.

Table 8-6  Description for Calling Party Number Type

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Party Number Type | Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national numbering plan type. Choose one of the following options:  
  - Cisco CallManager—The Cisco Unified Communications Manager sets the directory number type.  
  - Unknown—Choose when the dialing plan is unknown.  
  - National—Use when you are dialing within the dialing plan for your country.  
  - International—Use when you are dialing outside the dialing plan for your country.  
  - Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.  
In the following windows in Cisco Unified Communications Manager Administration, you can configure the Calling Party Number Type setting:  
  - Hunt List Detail Configuration—Call Routing > Route/Hunt > Hunt List (Add the hunt list; after you click **Save**, the Add Line Group button displays. To display the Hunt List Detail Configuration window, click the **Add Line Group** button.)  
  - Route Pattern Configuration—Call Routing > Route/Hunt > Route Pattern  
  - Hunt Pilot Configuration—Call Routing > Route/Hunt > Hunt Pilot  
  - Translation Pattern Configuration—Call Routing > Translation Pattern  
  - Calling Party Transformation Pattern Configuration—Call Routing > Transformation Pattern > Calling Party Transformation Pattern  
Tip In the Gateway and Trunk Configuration window, you can configure the Calling Party IE Number Type Unknown setting. If you can configure this setting and choose any other option except for Cisco CallManager, which is the default, your configuration for this field overwrites the Calling Party Number Type setting for the outgoing call through a particular gateway.

Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows

This section contains information on the following topics:

- Considerations for Configuring the Prefix Field, page 8-19
- Considerations for Configuring the Strip Digits Field, page 8-19
- Incoming Calling Party Number Settings, page 8-20
Considerations for Configuring the Prefix Field

Before you configure the prefix fields that are described in Table 8-7, consider the following information.

- In the Device Pool, Gateways, and Trunk Configuration windows, to delete the prefixes in all incoming calling party settings at the same time, click Clear Prefix Settings; to enter the default value for all incoming calling party settings at the same time, click Default Prefix Settings.

- If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.

- To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

- When the prefix gets applied to the incoming calling party number on the device, Cisco Unified Communications Manager includes the prefix in the calling party number field for all additional actions, such as supplementary services including call forwarding, call park, voice messaging, CDR data, and so on, that pertain to the call.

- If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix. (For example, the calling party number arrives empty because you chose Restricted from the Calling Line ID Presentation drop-down list box in the Route Pattern, Gateway, or Trunk Configuration windows.)

- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

- Configure the incoming prefix fields in conjunction with the strip digit fields; that is, if your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the fields in Table 8-7 to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

Before you configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number, consider the following information.

- You can either strip digits by configuring the Incoming Prefix service parameters in the Service Parameter Configuration window or by configuring the Strip Digits fields in the Device Pool, Gateway, or Trunk Configuration windows. For information on how to configure the service parameters for this functionality, see the “Setting the Service Parameters for Calling Party Normalization” section on page 8-15.
Chapter 8  Calling Party Normalization

Configuring Calling Party Normalization

If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.

To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

Be aware that Cisco Unified Communications Manager can strip up to 24 digits. If you enter a value that is larger than 24 in the field, for example, 26, Cisco Unified Communications Manager Administration does not allow the configuration.

If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix.

If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).

If you do not configure a value for the Strip Digits fields, Cisco Unified Communications Manager does not strip any digits from the calling party number.

If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Incoming Calling Party Number Settings

The settings in Table 8-7 display in the following windows in Cisco Unified Communications Manager Administration:

- Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device.
- Gateway (Device > Gateway)—Displays settings in the H.323 gateway configuration window and in the port windows (Gateway Configuration window) for MGCP (T1-PRI/BRI) and MGCP (E1-PRI/BRI).
- Trunk (Device > Trunk)—Displays all settings in all trunk configuration windows except the SIP trunk.

Tip

The SIP Trunk Configuration window only displays the Incoming Number settings, which is used for the Unknown calling party number type.

For configuration procedures for each configuration window, see the following sections:

- Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Configuring a Trunk, Cisco Unified Communications Manager Administration Guide
### Table 8-7  
Incoming Calling Party Number Settings for Device Pools, Gateways, and Trunks

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Prefix Setting</td>
<td>To delete all prefixes for all calling party number types, click <strong>Clear Prefix Settings</strong>.</td>
</tr>
<tr>
<td>Default Prefix Setting</td>
<td>To enter the default value for all prefix fields at the same time, click <strong>Default Prefix Settings</strong>.</td>
</tr>
<tr>
<td>National Number</td>
<td>Configure the following settings to globalize calling party numbers that use National for the Calling Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td>• Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>• Use Device Pool CSS—This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Table 8-7  Incoming Calling Party Number Settings for Device Pools, Gateways, and Trunks (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Number</td>
<td>Configure the following settings to globalize calling party numbers that use International for the Calling Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.</td>
</tr>
<tr>
<td>Tip</td>
<td>If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td>Tip To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.</td>
</tr>
<tr>
<td></td>
<td>• Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>• Use Device Pool CSS—This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td>Tip</td>
<td>Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.</td>
</tr>
</tbody>
</table>
### Configuring Calling Party Normalization

Subscriber Number Configure the following settings to globalize calling party numbers that use Subscriber for the Calling Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.

**Tip**
If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

**Tip**
To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

- **Use Device Pool CSS**—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device.

- **Calling Search Space**—This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Tip**
Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Number</td>
<td>Configure the following settings to globalize calling party numbers that use Subscriber for the Calling Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>- Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td>- Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.</td>
</tr>
<tr>
<td></td>
<td>- Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device.</td>
</tr>
<tr>
<td></td>
<td>- Calling Search Space—This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.</td>
</tr>
</tbody>
</table>
### Chapter 8      Calling Party Normalization

#### Configuring Calling Party Normalization

Unknown Number (does not display in the SIP Trunk Configuration window)

Configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.

**Tip**

If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes.

- **Use Device Pool CSS**—This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device.

- **Calling Search Space**—This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Tip**

Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Number</td>
<td>Configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.</td>
</tr>
<tr>
<td></td>
<td>• Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>• Use Device Pool CSS—This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
|                              | **Tip**
|                              | Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing. |
### Chapter 8  Calling Party Normalization

#### Configuring Calling Party Normalization

Before you configure the Calling Party Transformation CSS, make sure that you understand the steps that are required to localize the calling party number; for example, configuring the partition, configuring the calling search space, and so on. For more information, see the “Configuration Checklist for Calling Party Normalization” section on page 8-1.

Table 8-8 describes the various Calling Party Transformation CSS settings and lists the configuration windows in Cisco Unified Communications Manager Administration where you assign the settings.

---

**Table 8-7  Incoming Calling Party Number Settings for Device Pools, Gateways, and Trunks (continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Number (displays in the SIP Trunk Configuration window only)</td>
<td>SIP trunks support calling party number type of Unknown only. For SIP trunks only, configure the following settings to globalize calling party numbers that use Unknown for the Calling Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>– Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to 8 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> If the word, Default, displays in the Prefix field in the Gateway or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To configure the Strip Digits field in the Device Pool, Gateway, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.</td>
</tr>
<tr>
<td></td>
<td>– Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>– Use Device Pool CSS—This setting displays in the Gateway and Trunk Configuration windows, not the Device Pool Configuration window. Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device.</td>
</tr>
<tr>
<td></td>
<td>– Calling Search Space—This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.</td>
</tr>
</tbody>
</table>

---

**Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number**

Before you configure the Calling Party Transformation CSS, make sure that you understand the steps that are required to localize the calling party number; for example, configuring the partition, configuring the calling search space, and so on. For more information, see the “Configuration Checklist for Calling Party Normalization” section on page 8-1.

Table 8-8 describes the various Calling Party Transformation CSS settings and lists the configuration windows in Cisco Unified Communications Manager Administration where you assign the settings.
Providing Information to End Users

Depending on your configuration, a phone user may not need to edit the call log directory entry on the phone before placing a call. Depending on your configuration, the phone user may see the international escape character, +, in the call log directories on the phone.

### Table 8-8 Configuring the Calling Party Transformation CSS to Localize the Calling Party Number

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Party Transformation CSS</td>
<td>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</td>
</tr>
<tr>
<td>Use Device Pool Calling Party Transformation CSS</td>
<td>To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the device configuration window.</td>
</tr>
</tbody>
</table>

All phone device types, CTI route points, gateways, remote destination profiles, and trunks in Cisco Unified Communications Manager Administration can localize the calling party number for themselves; therefore, you can access this setting in the following windows in Cisco Unified Communications Manager Administration:

- Device Pool (System > Device Pool)
- Phone (Device > Phone)
- CTI Route Points (Device > CTI Route Point)
- Gateway (Device > Gateway)—Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window.
- Trunk (Device > Trunk)
- Remote Destination Profile (Device > Device Settings > Remote Destination Profile)
Related Topics

- Globalizing the Calling Party Number, page 8-5
- Localizing the Calling Party Number, page 8-7
- Mapping the Global Party Calling Number to Its Local Variant, page 8-9
- System Requirements, page 8-10
- Interactions and Restrictions, page 8-10
- Installing and Activating Calling Party Normalization, page 8-15
- Configuration Checklist for Calling Party Normalization, page 8-1
- Setting the Service Parameters for Calling Party Normalization, page 8-15
- Configuring the Calling Party Number Type, page 8-17
- Configuring the Incoming Calling Party Settings in the Device Pool, Gateway, or Trunk Configuration Windows, page 8-18
- Applying the Calling Party Transformation Calling Search Spaces (CSS) to Localize the Calling Party Number, page 8-25
- Providing Information to End Users, page 8-26
- Device Mobility, page 20-1
- Using the International Escape Character +, Cisco Unified Communications Manager System Guide

Additional Cisco Documentation

- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified IP Phone documentation that supports your phone model and this version of Cisco Unified Communications Manager
Cisco Extension Mobility

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

Extension mobility functionality extends to most Cisco Unified IP Phones. You can configure each Cisco Unified IP Phone to support Cisco Extension Mobility by using the Default Device Profile window in Cisco Unified Communications Manager Administration. This allows users who do not have a user device profile for a particular Cisco Unified IP Phone to use Cisco Extension Mobility with that phone.

Note
Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported.

This chapter provides the following information about Cisco Extension Mobility:

- Configuration Checklist for Cisco Extension Mobility, page 9-1
- Introducing Cisco Extension Mobility, page 9-5
- System Requirements for Cisco Extension Mobility, page 9-13
- Interactions and Restrictions, page 9-14
- Installing Cisco Extension Mobility for the First Time, page 9-17
- Configuring Cisco Extension Mobility, page 9-17
- Providing Information to Cisco Extension Mobility Users, page 9-35
- Related Topics, page 9-35

Configuration Checklist for Cisco Extension Mobility

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

Extension mobility functionality extends to most Cisco Unified IP Phones. You can configure each Cisco Unified IP Phone to support Cisco Extension Mobility by using the Default Device Profile window in Cisco Unified Communications Manager Administration. This allows users who do not have a user device profile for a particular Cisco Unified IP Phone to use Cisco Extension Mobility with that phone.

Note
Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported.
Perform the procedures in the order shown in Table 9-1 to configure Cisco Extension Mobility. For more information on Cisco Extension Mobility, see the “Introducing Cisco Extension Mobility” section on page 9-5 and the “Related Topics” section on page 9-35.

Table 9-1  Configuration Checklist for Cisco Extension Mobility

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Using Cisco Unified Serviceability, choose <strong>Tools &gt; Service Activation</strong> to activate the Cisco Extension Mobility service.</td>
<td>For information on service activation, see the <em>Cisco Unified Serviceability Administration Guide</em>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>To disable the extension mobility service on any node, you must first deactivate the service for that node in Service Activation.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>When a change in activation or deactivation of the Cisco Extension Mobility service occurs, on any node, the database tables get updated with information that is required to build the service URLs. The database tables also get updated when the extension mobility service parameters get modified. The EMApp service handles the change notification.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 9-1 Configuration Checklist for Cisco Extension Mobility (continued)

| Step 2 | Create the Cisco Extension Mobility Service.  
<table>
<thead>
<tr>
<th>Summary steps include</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| • Choose Device > Device Settings > Phone Services.  
• Enter the service name (such as, Extension Mobility Service or EM).  
• Enter the following URL:  
```
http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#
```  
**Note** If you should enter the URL incorrectly and subscribe the wrong service to the phones, you can correct the URL, save it, and press Update Subscriptions or correct the URL and resubscribe each phone to which the wrong service was subscribed.  
• Select values for Service Category and Service Type.  
  - For Service Category select “XML Service”.  
  - For Service Type, select “Standard IP Phone Service.”  
• Enter a value for Service Vendor (Java MIDlet services only).  
• Click Save.  
**Note** For Java MIDlet services, the service name and service vendor must exactly match the values that are defined in the Java Application Descriptor (JAD) file. | Adding the Cisco Extension Mobility Service, page 9-19. |

| Step 3 | Configure administration parameters. | Setting the Service Parameters, page 9-20 |

| Step 4 | Create a default device profile for each phone type that you want to support Cisco Extension Mobility. | Creating a Default Device Profile for Each Cisco Unified IP Phone Type, page 9-26 |
### Table 9-1  Configuration Checklist for Cisco Extension Mobility (continued)

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
|       | Create the user device profile for a user. | Creating the Device Profile for a User, page 9-28  
|       | Summary steps include: | Intercom Directory Number Configuration, page 28-28 |
|       | • Choose Device > Device Settings >Device Profile and click Add New. | |
|       | • Enter the Device Type. | |
|       | • Enter the Device Profile Name, choose the phone button template, and click Save. | |
|       | • Enter the directory numbers (DNs) and required information and click Save. Repeat for all DNs. | |
|       | • To enable intercom lines for this device profile, configure intercom directory numbers (DNs) for this device profile. You configure an intercom DN in the Intercom Directory Number Configuration window, which you can also access by choosing Call Routing > Intercom > Intercom Directory Number. You must designate a Default Activated Device in the Intercom Directory Number Settings pane for an intercom DN to be active. | |
|       | • To subscribe the device profile to Cisco Extension Mobility, on the Device Profile Configuration Window, from the related links drop-down list (in the upper right corner of the window), choose “Subscribe/Unsubscribe Services” and click Go. | |
|       | **Note** Subscribe the directory number and the device profile the same Extension Mobility service. | |
| Step 6 | Associate a user device profile to a user. | Associating a User Device Profile to a User, page 9-31 |
|       | Summary steps include: | |
|       | • Choose User Management > End User and click Add New; enter user information. | |
|       | • In Extension Mobility Available Profiles, choose the user device profile that you created in Step 5 and click the down arrow; this places the service that you chose in the Controlled Profiles box. | |
|       | • Click Save. | |
Introducing Cisco Extension Mobility

The following sections will help you to understand Cisco Extension Mobility, so you can configure and troubleshoot the feature:

- Understanding Device Profiles, page 9-5
- Overview of Cisco Extension Mobility, page 9-6
- Login and Logout Behavior, page 9-8
- Login Call Flow, page 9-9
- Logout Call Flow, page 9-10
- Extension Mobility Equivalency, page 9-11

Understanding Device Profiles

A device profile defines the attributes of a particular device. A device profile includes information such as the phone template, user locale, subscribed services, and speed dials.

The device profile does not get associated with a physical phone. It includes all the properties of a device except those that are explicitly tied to a device, such as MAC address or directory URL.
Introducing Cisco Extension Mobility

When a device profile has been loaded onto a device, the device adopts the attributes of that device profile.

User Device Profile

As system administrator, you configure a user device profile for each individual user. Using the Cisco Unified CM User Options window, a user can access this profile and make changes, such as adding a service. You can add, modify or delete a user device profile in Cisco Unified Communications Manager Administration.

When a user logs in to a phone that is configured for Cisco Extension Mobility and the user has a user device profile that is configured for that phone, the user device profile replaces the existing configuration of the device.

When a user logs out, the logout profile replaces the user device profile.

Default Device Profile

You can configure a default device profile for each Cisco Unified IP Phone that you want to support Cisco Extension Mobility. The phone takes on the default device profile whenever a user logs in to a phone for which that user does not have a user device profile.

A default device profile includes device type (phone), user locale, phone button template, softkey template, and multilevel precedence and preemption (MLPP) information.

You create a default device profile by using the Default Device Profile Configuration window (Device > Device Settings > Default Device Profile). A phone can have zero or one default device profile. The maximum number of default device profiles cannot exceed the number of phones that support Cisco Extension Mobility.

Overview of Cisco Extension Mobility

Cisco Extension Mobility (an XML-based authentication feature) comprises the Cisco Extension Mobility application service and the Cisco Extension Mobility service. You need to activate the Cisco Extension Mobility service from Cisco Unified Serviceability to enable EM.

The Cisco Extension Mobility service runs as an application on the Cisco Tomcat Web Service.

You can activate/deactivate services from Cisco Unified Serviceability > Service Activation. See the Cisco Unified Serviceability Administration Guide for more information.

---

**Note**

Cisco Extension Mobility works on phones within a single Cisco Unified Communications Manager cluster only.

---

**Note**

Cisco Extension Mobility Cross Cluster works on phones that are located in different Cisco Unified Communications Manager clusters. For details about the Cisco Extension Mobility Cross Cluster feature, see the “Cisco Extension Mobility Cross Cluster” chapter.
You can use Cisco Unified Communications Manager Administration to start the Cisco Extension Mobility services (in Cisco Unified Serviceability administration), define how the features will work in your system (using the Service Parameters window [System > Service Parameters]), and define the phones that will support the feature (using the Default Device Profile window [Device > Device Settings > Default Device Profile]).

As system administrator, you configure a user device profile for each individual user. Using the Cisco Unified CM User Options window, a user can access this profile and make changes, such as adding a service like Cisco Extension Mobility.

Users access Cisco Extension Mobility by pressing the Services or Applications button on a Cisco Unified IP Phone and then entering login information in the form of a Cisco Unified Communications Manager UserID and a Personal Identification Number (PIN). If a user has more than one user device profile, a prompt displays on the phone and asks the user to choose a device profile for use with Cisco Extension Mobility.

If the user phone is subscribed to the Change Credential IP Phone service, the user can use the Change Credential IP Phone service to change the user PIN.

When a user logs in, the Cisco Extension Mobility application receives the XML-over-HTTP request for user authentication and verifies the information against the Cisco Unified Communications Manager Directory. (See Figure 9-1.)

**Figure 9-1 Cisco Extension Mobility**

![Diagram of Cisco Extension Mobility](image)

On authentication, if the login profile matches the login device (that is, the user has a user device profile that is configured for a Cisco Unified IP Phone 7975 and logs into a Cisco Unified IP Phone 7975), Cisco Extension Mobility behaves as follows:

- The phone automatically reconfigures with the individual user device profile information.
  
  If the user has one user device profile, the system uses this profile. If the user has more than one user device profile, the user can choose the user device profile that will be used from a list.

- The user can access all the services that the user configured on the device profile.
If that same user logs into a Cisco Unified IP Phone where the user does not have a configured user device profile, the login profile will not match the login device on authentication. In this scenario, the system loads the default device profile for that phone model onto the phone, and Cisco Extension Mobility works as described here:

- The system copies all device-independent configuration (that is, user hold audio source, user locale, userid, speed dials, and directory number configuration except for the setting “line setting for this device”) from the user device profile to the login device.
- The system uses the default device profile for that phone for phone template and softkey template configuration and, if the phone can support addon modules, for the addon module.
- If the login device supports feature safe on the phone button template and if the phone template that is configured in the login profile matches the number of buttons, the system uses the phone template from the login profile. Otherwise, the system uses the default device profile for the phone to configure the phone template.
- If the phone supports Cisco Unified IP Phone Services and they are configured, the system copies the services from the user device profile.

If the user device profile does not have Cisco Unified IP Phone Services configured, the system uses the Cisco Unified IP Phone Services that are configured in the default device profile for the login device that is accessed during login. If parameters exist for the subscriber service, the system copies the parameters from the default device profile, and the parameters may not reflect the correct information.

For example, the following scenarios occur when a user who has a user device profile that is configured for Cisco Unified IP Phone 7975 logs in to a Cisco Unified IP Phone 7906, and the default device profile is loaded on the phone.

- The user can access the user hold audio source, user locale, userid, speed dials and directory number configuration. The user cannot access phone line setting; the system configured the phone line setting from the default device profile that is configured for the Cisco Unified IP Phone 7906.
- The user can access the phone template and the softkey template of the Cisco Unified IP Phone 7906.
- The user cannot access an addon module because Cisco Unified IP Phone 7906 does not support it.
- The user can access Cisco Unified IP Phone Services if they are configured for the Cisco Unified IP Phone 7906, but the parameters from the subscriber services will reflect the default device profile, not the parameters that the user chose on the Cisco Unified CM User Options window.

Users log out of Cisco Extension Mobility by pressing the Services button and choosing logout. If users do not log out themselves, the system will automatically log them out if you configured the Service Parameters to do so, or the next user of the phone can log out the previous user. After logout, Cisco Unified Communications Manager sends the logout profile to the phone and restarts the phone.

### Login and Logout Behavior

This section describes how login and logout works from the user perspective. Use this information to respond to questions or problems that users may encounter.

- Cisco recommends that you direct your users to log in to their phones at the beginning of the workday. This practice ensures that the user device profile gets loaded on the phone.
- If users make changes to their profiles on the Cisco Unified CM User Options window, the changes will apply the next time that they log in.
- The system does not apply the change if the user is already logged in.
• If the User Locale that is associated with the login user or profile does not match the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file gets rebuilt. Addon module mismatches between profile and device may generate the same behavior.

• Cisco Extension Mobility supports a maximum of 250 login or logout operations per minute (or 15,000 operations per hour). Remember that these operations are sequential, not concurrent. (Some devices may support more login or logout operations per hour.)

• You can establish a time limit, so Cisco Extension Mobility automatically logs out users, after a certain time, throughout the cluster. At the Enforce Maximum Login Time, choose True to specify a maximum time for logins and then set the maximum login time.

See the “Setting the Service Parameters” section on page 9-20.

• You can set the service parameter to allow for multiple logins. If you set multiple login not allowed, Cisco Extension Mobility supports only one login at a time for a user. Subsequent logins on other devices will fail until the user logs out on the first device.

• If Auto Logout is not enabled and if users forget to log out of a phone, as system administrator, you can log them out. Another user also can log them out when the second user tries to log in to that phone.

• If users are logged out of a Cisco Unified IP Phone that has the Cisco Extension Mobility feature configured for it, depending on the logout profile, they may not be able to check voice-messaging systems from that phone until they log in. If they receive a busy signal after pressing the Messages button or any key on the touchtone key pad, they must log in before using the phone.

• Users can log in to a phone that is off hook; however, their Cisco Unified IP Phone will not assume their settings until they go on hook. When they go on hook after logging in, their phone will display a “Resetting...” message, and their phone settings will be available from that phone.

• The Cisco Extension Mobility profile of a user does not maintain ring type, contrast settings, and volume settings; users configure these settings directly on the Cisco Unified IP Phone.

• When a Cisco Extension Mobility user logs out of a device, all Call Back services that are active on the Cisco Extension Mobility user automatically cancel.

Additional Information
See the Related Topics, page 9-35.

Login Call Flow

This section describes the flow of events for the Cisco Extension Mobility login from a system perspective. Understanding the call flow will help you troubleshoot problems that you may have with the feature.

1. A user presses the Services or Applications button on the Cisco Unified IP Phone and requests to log in. This action invokes a URL for the Cisco Extension Mobility application.

2. The application determines the URL of the service.

3. The Cisco Extension Mobility application sends a formatted XML/HTTP query to the Cisco Extension Mobility service to determine the state of the phone.

4. The application prompts the user for UserID and PIN. The user enters the UserID and PIN and presses the Submit softkey.

5. The phone performs an HTTP request, and the application tries to authenticate the UserID and PIN.
6. If the UserID and PIN cannot be authenticated, the phone displays “Authentication Error.”
   If the UserID and PIN are authenticated, the application queries the Cisco Unified Communications Manager Database to get the list of device profiles that are associated with the user.
7. The directory responds with the list of the user device profile(s). If the list has more than one entry, the phone displays the device profiles from which the user can choose.
8. When the user chooses an entry from this list (or if the list has only one entry), the application generates the XML.
9. The application posts, via HTTP, the generated XML login request to the service URL. (The application determined the service URL in Step 2.)
10. The service responds in a defined XML format to the request with a restart to load the user device profile (that indicates success) or with a failure message.
11. The application returns the correct notification to the device. The phone restarts with the user device profile.
12. In the Phone Configuration window (Device > Phone) of Cisco Unified Communications Manager Administration, the Current End User Profile and the Current Device Profile, along with links to the applicable End User Profile and Device Profile configuration windows display.

**Note**  
In the Phone Configuration window, the line number of the device does not change when a user logs in to the phone. It continues to display the line number that is assigned to the phone when no user is logged in.

**Additional Information**  
See the Related Topics, page 9-35.

## Logout Call Flow

This section describes the flow of events for the Cisco Extension Mobility logout from a system perspective. Understanding the call flow will help you troubleshoot any problems that you may have with the Cisco Extension Mobility feature.

1. A user presses the Services or Applications button on the Cisco Unified IP Phone and requests to log out. This action invokes a URL for the Cisco Extension Mobility application.
2. The application determines the URL of the service.

**Note**  
Cisco Extension Mobility looks up the URL in the Cisco Unified Communications Manager Directory on the first instance only; the system then stores the URL as a static variable.

3. The application generates the XML to query the Cisco Extension Mobility service for the current state of the device.
4. The service responds to the application with the current state of device; for example, `<userID>` is logged in.
5. The application prompts the user to confirm that the user wants to log out.
6. When the user presses the Yes softkey to confirm that the user wants to log out, the application generates XML for the logout operation.
7. The application posts, via HTTP, the generated XML login request to the service URL. (The application determined the service URL in Step 2.)

8. In the case of a successful operation, the phone will restart and load the appropriate device profile. If a failure occurs, a message gets sent to the phone.

9. The application parses the received XML and creates an XML response message.

10. The XML gets returned as a suitable notification to the device, and the phone restarts to load the original user profile or logout profile.

11. In the Phone Configuration window (Device > Phone) of Cisco Unified Communications Manager Administration, you (the administrator) will no longer see a Current End User Profile and Current Device Profile.

Note: In the Phone Configuration window, the line number of the device does not change when a user logs out from the phone. It continues to display the line number that is assigned to the phone when no user is logged in.

Extension Mobility Equivalency

Cisco Extension Mobility (EM) equivalency eliminates the phone-model dependency of phone button templates. The following factors determine the model equivalency among the various phones:

- Various features that the phone models support
- Number of buttons that the phone models support

EM equivalency supports these features for the Cisco Unified IP Phones:

- Feature Safe on Phone Button Template—Phones can use any phone button template that has the same number of line buttons that the phone model supports.
- Size Safe on Phone Button Template—This feature allows the user to use any phone button template that is configured on the system.

Cisco Unified Communications Manager enhances the existing Extension Mobility (EM) equivalency mechanism to work across phone types as follows:

- Feature Safe on Phone Button Template—For both SCCP and SIP protocols, the following Cisco Unified IP Phone models support the Feature Safe feature: 7931, 7941, 7941G-GE, 7942, 7945, 7961G-GE, 7962, 7965, 7975. For the SIP protocol only, the following Cisco Unified IP Phone models support the Feature Safe feature: 8961, 9951, 9971.

Note: Be aware that the Feature Safe on Phone Button Template feature does not support using an EM profile that is configured for a newer model on the Cisco Unified IP Phone 7960 or 7940.

- Size Safe on Phone Button Template—For both SCCP and SIP protocols, the following Cisco Unified IP Phone models support the Size Safe feature: 7906, 7911, 7931, 7941, 7941G-GE, 7942, 7945, 7961, 7961G-GE, 7962, 7965, 7975.

The enhancement works for all phone models that are equivalent and requires no administration tasks to activate.
Introducing Cisco Extension Mobility

The list of supported phone models varies per version and device pack. Log in to Cisco Unified Reporting to obtain the complete list of phone models that support these features in your installation. Within Cisco Unified Reporting, choose the Unified CM Phone Feature List system report. When generating this system report, specify All in the Product drop-down list box. In the Feature drop-down list box, specify either Feature Safe on Phone Template or Size Safe on Phone Template.

Feature Safe Configuration Scenario

1. Use the User Device Profile Configuration window (Device > Device Settings > Device Profile) to create a 7975 user device profile. Name the 7965 user device profile User Profile Test and configure the profile to use the 7965 phone button template and to include the following lines:
   - DN: 1050, 1051, and 1052
   - Speed Dial: 5051, 5052, 5053, 5054, and 5055

2. Use the User Configuration window (User Management > End User) to create a user. Name the user cisco and associate the User Profile Test user device profile with this user.

3. Use the Phone Configuration window (Device > Phone) to configure a Cisco Unified IP Phone 7965 and a Cisco Unified IP Phone 7975 with extension mobility. Configure each phone to use the Standard phone button template.

4. When the user logs in to a Cisco Unified IP Phone 7965 with the User Profile Test user device profile, all the lines (DNs) and speed dials display on the phone screen.

5. When the user logs in to a Cisco Unified IP Phone 7975 with the User Profile Test user device profile, because the phone supports feature safe on the phone button template, all the lines (DNs) and speed dials display on the phone screen.

Size Safe Functionality

If a phone model supports Size Safe on Phone Button Template, any phone button template can associate with that phone model. The actual phone button layout that displays on the phone shows the same order as the defined phone button template. If the phone model has more buttons than the phone button template, all defined buttons display. If the phone model has fewer buttons than the defined phone button template, only the buttons that are available on the phone display.

For example, a Cisco Unified IP Phone 7961 phone button template defines the following buttons:

• Line1
• Line2
• SD1
• SD2
• Line3
• Line4

When this phone button template gets assigned to a Cisco Unified IP Phone 7942, the actual phone button layout shows the following:

• Line1
• Line2

The rest of the template does not display because the buttons are not available.
When this phone button template gets assigned to a Cisco Unified IP Phone 7975, that actual phone button layout shows the following:

- Line1
- Line2
- SD1
- SD2
- Line3
- Line4
- Undefined
- Undefined

Thus, if a phone model supports the Size Safe on Phone Button Template feature, regardless of the login profile model, the user always sees the same order of the phone button template layout as that which gets defined with the login profile.

**Additional Information**

See the Related Topics, page 9-35.

## System Requirements for Cisco Extension Mobility

### Software Components

This version of Cisco Extension Mobility requires the following software components to operate:

- Cisco Unified Communications Manager 8.0 or later

**Note**

Cisco Extension Mobility installs automatically on the same server with Cisco Unified Communications Manager. You do not require an additional server. Cisco Extension Mobility can run on any server in a Cisco Unified Communications Manager cluster.

- Netscape 7.1, Internet Explorer 6, or Internet Explorer 7 for Cisco Unified Communications Manager Administration
- Ensure the TFTP server is reachable. You can optionally install TFTP and Cisco Unified Communications Manager on the same server.

Extension mobility functionality extends to most Cisco Unified IP Phones. Check the Cisco Unified IP Phone documentation to verify that Cisco Extension Mobility is supported. See the following URLs:


### Backward Compatibility for Call Forward All Calling Search Space

An enhancement to Call Forward All calling search space (CSS) allows customers who are using Cisco Extension Mobility to upgrade to later releases of Cisco Unified Communications Manager without loss of functionality.
The CFA CSS Activation Policy service parameter supports this enhancement. In the Service Parameter Configuration window (System > Service Parameters), this parameter displays in the Clusterwide Parameters (Feature - Forward) section with two options.

- With Configured CSS (default)
- With Activating Device/Line CSS

For more information about configuration options for Call Forward All, see the “Directory Number Configuration” chapter in the Cisco Unified Communications Manager Administration Guide and the “Understanding Directory Numbers” chapter in the Cisco Unified Communications Manager System Guide.

Additional Information
See the Related Topics, page 9-35

Interactions and Restrictions

Use the following sections to understand how Cisco Extension Mobility interacts with other Cisco Unified Communications Manager services and to understand restrictions that apply to Cisco Extension Mobility:

- Interactions, page 9-14
- Restrictions, page 9-16

Interactions

The following sections describe how Cisco Extension Mobility interacts with Cisco Unified Communications Manager applications:

- Cisco Unified Communications Manager Services That Are Running on the Same Server, page 9-14
- Bulk Administration Tool, page 9-14
- Cisco Unified Communications Manager Assistant, page 9-15
- Call Display Restrictions, page 9-15
- Intercom, page 9-15
- Internet Protocol Version 6 (IPv6), page 9-16

Cisco Unified Communications Manager Services That Are Running on the Same Server

Cisco Extension Mobility can run on the same Cisco Unified Communications Manager server with Cisco Unified Communications Manager Assistant and CDR Analysis and Reporting (CAR).

Bulk Administration Tool

You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco Extension Mobility at one time. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.
Cisco Unified Communications Manager Assistant

A manager who uses Cisco Extension Mobility can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs into the Cisco Unified IP Phone by using Cisco Extension Mobility and then chooses the Cisco IP Manager Assistant service. When the Cisco IP Manager Assistant service starts, the manager can access assistants and all Cisco Unified Communications Manager Assistant features (such as call filtering and Do Not Disturb). For more information about Cisco Unified Communications Manager Assistant, see the “Cisco Unified Communications Manager Assistant With Proxy Line Support” chapter.

Call Display Restrictions

When you enable Call Display Restrictions with Cisco Extension Mobility, Cisco Extension Mobility functions as usual: when a user is logged in to the device, the presentation or restriction of the call information depends on the user device profile that is associated with that user. When the user logs out, the presentation or restriction of the call information depends on the configuration that is defined for that phone type in the Phone Configuration window (Device > Phone).

To use Call Display restrictions with Cisco Extension Mobility, enable the Ignore Presentation Indicators (internal calls only) in both the Device Profile Configuration window (see the “Creating the Device Profile for a User” section on page 9-28) and the Phone Configuration window (see the “Subscribing Cisco Unified IP Phones to Cisco Extension Mobility” section on page 9-32).

For more information about the Call Display Restrictions features, see the “Call Display Restrictions” chapter.

Intercom

Cisco Extension Mobility supports the Intercom feature. To do so, Cisco Extension Mobility uses a default device that is configured for an intercom line. An intercom line gets presented only on the default device.

You can assign an intercom line to a device profile. When a user logs on to a device that is not the default device, the intercom line does not get presented.

The following additional considerations apply to intercom for Cisco Extension Mobility:

- For an existing intercom line that is assigned to a device, migration from a Release 6.0(1) of Cisco Unified Communications Manager to Release 6.1(1) or later automatically designates the intercom default device for that intercom line.
- When Cisco Unified Communications Manager assigns an intercom line to a device and the default device value is empty, the current device gets selected as the default device.
- When assignment of an intercom DN takes place programatically through AXL, ensure the intercom DN is updated separately by using Cisco Unified Communications Manager Administration to set the default device.
- When deletion of a device that is set as the intercom default device for an intercom line occurs, the deletion completes, and the intercom default device will no longer be set to the deleted device.
Internet Protocol Version 6 (IPv6)

Cisco Extension Mobility supports IPv4, so you cannot use phones with an IP Addressing Mode of IPv6 Only for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

Restrictions

The following restrictions apply to Cisco Extension Mobility:

- Cisco Extension Mobility works on phones within a single Cisco Unified Communications Manager cluster only.
- The characters that display when a user logs in depend on the current locale of the phone. For example, if the phone is currently in the English locale (based on the Logout profile of the phone), the user can only enter English characters in the UserID.
- Cisco Extension Mobility supports a limited number of special characters that can be entered on the phone for the login user ID. These characters include . (period), @, ~, *, &, %, #, +, $, \, the Euro sign, and the pound sterling sign.
- If the User Locale that is associated with the login user or profile is not the same as the locale or device, after a successful login, the phone will perform a restart followed by a reset. This occurs because the phone configuration file gets rebuilt. Addon module mismatches between profile and device may cause the same behavior.
- Cisco Extension Mobility requires a physical Cisco Unified IP Phone for login. Users of office phones that are configured with Cisco Extension Mobility cannot log in to their phones remotely.
- When a Cisco Extension Mobility user logs out of a device, all Call Back services that are active for the Cisco Extension Mobility user automatically cancel.
- When a migration from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager Release 6.0 (or later) is done, the phones do not display the last login user IDs until users log in for the first time after the migration. When the service parameter “Remember the Last User Logged In” gets set to True, Cisco Extension Mobility displays the previous login user ID whenever the user logs in to the phone. This occurs based on a file on the hard disk. For the migration from Release 4.x to Release 6.0 (or later), this file does not get migrated to the database; therefore, the user ID of the previous login user does not display.
- If Cisco Extension Mobility gets stopped or restarted, the system does not auto log out users who are already logged in after the expiration of logout interval. For those phones, auto-logout happens only once in a day. You can manually log out these users from either the phones or from Cisco Unified Communications Manager Administration.
- Standard Extension Mobility (EM) Authentication Proxy Rights specifies both a standard role and a standard user group that are intended for use by applications that interact with Cisco Extension Mobility. Authentication by proxy does not support end-user authentication by proxy. Although you can add an end user to the Standard EM Authentication Proxy Rights user group, that end user does not get authorized to authenticate by proxy.
- Cisco Extension Mobility maintains a cache of all logged on user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user gets validated with information from the cache. This means that, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords get recognized.
Installing Cisco Extension Mobility for the First Time

When you install Cisco Unified Communications Manager, make sure that you also install the Cisco Unified Communications Manager Locale Installer on every server in the cluster. Installing the Locale Installer ensures that you have the latest translated text that is available for user windows and phone displays. For more information, see the *Cisco Unified Communications Operating System Administration Guide*.

Now, perform the procedures in the “Configuring Cisco Extension Mobility” section on page 9-17.

**Additional Information**

See the Related Topics, page 9-35

Configuring Cisco Extension Mobility

This section contains information on the following topics:

- Configuration Guidelines, page 9-17
- Configuration Example 1, page 9-18
- Configuration Example 2, page 9-18
- Adding the Cisco Extension Mobility Service, page 9-19
- Setting the Service Parameters, page 9-20
- Creating a Default Device Profile for Each Cisco Unified IP Phone Type, page 9-26
- Creating the Device Profile for a User, page 9-28
- Associating a User Device Profile to a User, page 9-31
- Subscribing Cisco Unified IP Phones to Cisco Extension Mobility, page 9-32
- Configuring the Change Credential IP Phone Service, page 9-33

**Tip**

Before you configure Cisco Extension Mobility, review the “Configuration Checklist for Cisco Extension Mobility” section on page 9-1.

Configuration Guidelines

To avoid problems with deploying Cisco Extension Mobility, be sure to follow these configuration guidelines:

- Configure a Default Device Profile for each Cisco Unified IP Phone in a cluster that you want to support Cisco Extension Mobility.

- If you want to enable all phones within a Cisco Unified Communications Manager cluster for Cisco Extension Mobility, do not allow the users to control these phones.
  - In this scenario, when users go to their Cisco Unified CM User Options window to change their services, they must choose the Device Profiles option from the Select a device to configure drop-down list box. They cannot control an individual phone nor modify the settings for an individual phone.
- As administrator, you can change the services for a phone by using Cisco Unified Communications Manager Administration. After making the changes, if you update on the main window (not the popup menu), you must reset the phone for the changes to take effect. This action ensures that the new snapshot gets stored as the logout profile.

- If a particular user controls a device, for example, the user office phone, do not allow anyone else to log in to that device.

Caution

The Cisco Extension Mobility feature does not operate properly if you allow users to access the assigned phone of another user.

- For information on Cisco Extension Mobility redundancy, see the Cisco Unified Communications Solution Reference Network Design (SRND) that is located at http://www.cisco.com/go/srnd.

Additional Information

See the Related Topics, page 9-35.

Configuration Example 1

In a typical Cisco Extension Mobility scenario,

- All employees represent users of Cisco Extension Mobility.
- All users have a user device profile.
- Users do not control individual phones, and they cannot modify settings for an individual phone.
- Before a user can use a phone, the user needs to log in.
- Users can access common devices, such as lobby phones, conference room phones, and cubicle phones that are meant to be shared.
- When users go to their Cisco Unified CM User Options window to change services or speed dials, they can choose only their device profiles from the “Select a device to configure” drop-down menu. This method ensures that changes that users make to their services will follow them to any Cisco Unified IP Phone after they log in.

Configuration Example 2

In another typical Cisco Extension Mobility scenario,

- Each user has an assigned phone.
- Each user has a device profile that follows the user to every device to which the user logs in.
- Each user can access common devices, such as lobby phones, conference room phones, and cubicle phones that are configured to be shared.
- In this scenario, no one can use the assigned phone of anyone else.

Additional Information

See the Related Topics, page 9-35.
Adding the Cisco Extension Mobility Service

Add the Cisco Extension Mobility service as a new Cisco Unified IP Phone Service. Configure a name, description, and the URL for the Cisco Extension Mobility service.

Tip
When you subscribe devices to the Cisco Extension Mobility service, an error results if you click Update Subscriptions more than once. When you update many phones, it can take some time for the changes to propagate to all devices. You must click Update Subscriptions only once and wait for this propagation to complete.

To add the Cisco Extension Mobility service, perform the following steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Phone Services.
Step 2 Click Add New.
Step 3 At the Service Name field, enter a name for the service.
   The user receives this name on the phone when the user presses the Services button. Use a meaningful name; for example, Extension Mobility or EM. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file.
Step 4 At the ASCII Service Name field, enter the name of the service to display if the phone cannot display Unicode.
Step 5 Enter the Service URL field as it displays in the following example:
   http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#
   where IP Address of Extension Mobility server specifies the IP Address of the Cisco Unified Communications Manager where Cisco Extension Mobility Application is activated and running.
   For example:
   http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#
   Tip
   To provide redundancy for the Cisco Unified IP Phone Service, create a Cisco Unified IP Phone Service that uses the host name rather than the IP address. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.
Step 6 At the Service Category field, select whether the service is based on XML or Java MIDlet.
Step 7 At the Service Type field, select whether the service will be provisioned to the Services, Directories, or Messages button.
Step 8 For Java MIDlet services only, at the Service Vendor field, enter the service vendor that exactly matches the vendor that is defined in the JAD file. You can leave this field blank for XML services.
   Note
   Be aware that entering a value for Service Version is not required. If you enter a value for a Java MIDlet service, the value must exactly match the version that is defined in the JAD file.
Step 9  Click Save.

Additional Information
See the Related Topics, page 9-35.

Setting the Service Parameters

Set the service parameters to define how the Cisco Extension Mobility service will work across a Cisco Unified Communications Manager cluster.

Be sure that you activate the Cisco Extension Mobility service before you configure the service parameters. See the Cisco Unified Serviceability Administration Guide for information about using Cisco Unified Serviceability.

To set the Service Parameters for Cisco Extension Mobility, choose System > Service Parameters in Cisco Unified Communications Manager Administration; choose the server that is running the Cisco Extension Mobility service, and then Cisco Extension Mobility. To display all service parameters, click Advanced. After you configure the service parameters, click Save.

Table 9-2 describes the Cisco Extension Mobility service parameters.

Note
Service parameters with “intra-cluster” in the name apply to the Cisco Extension Mobility feature. Service parameters with “inter-cluster” in the name apply only to the Cisco Extension Mobility Cross Cluster feature.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enforce Intra-cluster Maximum Login Time     | Choose True to specify a maximum time for local logins. After this time, the system automatically logs out the device. Choosing False, which is the default setting, means that no maximum time for logins exists.  
To set an automatic logout, you must choose True for the Enforce Intra-cluster Maximum Login Time service parameter and also specify a system maximum login time for the Intra-cluster Maximum Login Time service parameter. Cisco Unified Communications Manager then uses the automatic logout service for all logins. |
| Intra-cluster Maximum Login Time             | This parameter specifies the maximum time that a user is allowed to be locally logged in to a device, such as 8:00 (8 hours) or :30 (30 minutes).  
The system ignores this parameter if the Enforce Intra-cluster Maximum Login Time parameter is set to False.  
Valid values specify between 0:01 and 168:00 in the format HHH:MM where HHH represents the number of hours and MM represents the number of minutes. |
Chapter 9  Cisco Extension Mobility

Configuring Cisco Extension Mobility

Table 9-2  Service Parameters for Cisco Extension Mobility Service (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-cluster Maximum Login Time</td>
<td>This field applies only to Extension Mobility Cross Cluster (EMCC) configuration. This parameter specifies the maximum time that a user is allowed to be remotely logged in to a device, such as 8:00 (8 hours) or :30 (30 minutes). EMCC always enforces auto logout based on this value, regardless of the value of Enforce Intra-cluster Maximum Login Time service parameter. Valid values specify between 0:00 and 168:00 in the format HHH:MM where HHH represents the number of hours and MM represents the number of minutes. (0:00 means indefinite logon: you will remain logged on without a maximum login time.)</td>
</tr>
<tr>
<td>Maximum Concurrent Requests</td>
<td>Tip In the Service Parameter Configuration window, click Advanced to display this service parameter. Specify the maximum number of login or logout operations that can occur simultaneously. This number prevents the Cisco Extension Mobility service from consuming excessive system resources. The default value, which specifies 5, addresses most scenarios adequately.</td>
</tr>
<tr>
<td>Intra-cluster Multiple Login Behavior</td>
<td>Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Multiple Logins Allowed—A user can log in to more than one device at a time.</td>
</tr>
<tr>
<td></td>
<td>• Multiple Logins Not Allowed—The second and subsequent login attempts after a user successfully logs in once will fail.</td>
</tr>
<tr>
<td></td>
<td>• Auto Logout—After a user logs in to a second device, the Cisco Unified Communications Manager automatically logs the user out of the first device. For EMCC, multiple logins are always allowed.</td>
</tr>
<tr>
<td>Alphanumeric User ID</td>
<td>Choose True to allow the user ID to contain alphanumeric characters. Choosing False allows the user ID to contain only numeric characters.</td>
</tr>
<tr>
<td></td>
<td>Note The Alphanumeric User ID parameter applies systemwide. You can have a mix of alphanumeric and numeric user IDs. The system supports only user IDs that can be entered by using the alphanumeric keypad. The case-sensitive userid field requires the characters to be lower case.</td>
</tr>
</tbody>
</table>
### Chapter 9  Cisco Extension Mobility

#### Configuring Cisco Extension Mobility

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remember the Last User Logged In</td>
<td>Choose the default value, <strong>False</strong>.</td>
</tr>
<tr>
<td></td>
<td>In a typical hoteling scenario, where users can come into any office and use any phone on a temporary basis, you should set this parameter to <strong>False</strong>.</td>
</tr>
<tr>
<td></td>
<td>A True setting specifies that the extension mobility application remembers the user ID of the last user that logged in to the phone. Use this setting in situations where individuals use their own phone on a regular basis, and no one else uses that phone.</td>
</tr>
<tr>
<td></td>
<td>For example, Cisco Extension Mobility could be used to enable the types of calls that are allowed from a phone. Individuals who are not logged in and who are using their office phone can make only internal or emergency calls. But after logging in using Cisco Extension Mobility, the user can make local, long-distance, and international calls. In this scenario, only this user regularly logs in to the phone. It makes sense to set the Cisco Extension Mobility to remember the last user ID that logged in, and you would set the field to <strong>True</strong>. When the field is set to True, all future logins will cause the user ID of the last successful logged-in user to automatically get filled in and remembered by Cisco Extension Mobility.</td>
</tr>
<tr>
<td>Clear Call Logs on Intra-cluster EM</td>
<td>Choose <strong>True</strong> to specify that the call logs are cleared during the Cisco Extension Mobility manual login/logout process.</td>
</tr>
<tr>
<td></td>
<td>While a user is using the Cisco Extension Mobility service on an IP phone, all calls (placed, received, or missed) appear in a call log and can be retrieved and seen on the IP phone display. To ensure user privacy by preventing other users of the same phone from seeing the call logs of the previous user, set the Clear Call Log service parameter to <strong>True</strong>. This ensures that the call logs get cleared when a successful login/logout occurs.</td>
</tr>
<tr>
<td></td>
<td>For Extension Mobility Cross-Cluster (EMCC), the call log is always cleared when the user logs in or out of a phone.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Call logs get cleared only during manual Cisco Extension Mobility login/logout. If a Cisco Extension Mobility logout occurs due to an automatic logout or any occurrence other than a manual logout, the call logs do not get cleared.</td>
</tr>
</tbody>
</table>
Chapter 9  Cisco Extension Mobility

Configuring Cisco Extension Mobility

Validate IP Address

Tip

In the Service Parameter Configuration window, click Advanced to display this service parameter.

This parameter specifies whether validation of the IP address of the source that is requesting login or logout occurs.

If the parameter specifies true, the IP address from which a Cisco Extension Mobility log in or log out request is made gets validated to ensure that it is a trusted IP address.

Validation gets first performed against the cache for the device to be logged in or logged out.

If the requesting source IP address is not found in cache, the IP address gets checked against the list of trusted IP addresses and host names specified in the Trusted List of IPs service parameter.

If the requesting source IP address is not present in the Trusted List of IPs service parameter, it is checked against the list of devices registered to Cisco Unified CallManager.

If the IP address of the requesting source is found in the cache or in the list of trusted IP addresses or is a registered device, the device is allowed to perform login or logout.

If the IP address is not found, the log in or log out attempt is blocked. If the parameter specifies false, the Cisco Extension Mobility log in or log out request does not get validated.

Validation of IP addresses may increase the time required to log in or log out a device, but it offers an additional layer of security in the effort to prevent unauthorized log in or log out attempts, especially when used in conjunction with log ins from separate trusted proxy servers for remote devices.

Trusted List of IPs

Tip

In the Service Parameter Configuration window, click Advanced to display this service parameter.

This parameter displays as a text box (maximum length - 1024 characters). You can enter strings of trusted IP addresses or host names, separated by semi-colons, in the text box. IP address ranges and regular expressions do not get supported.

Allow Proxy

Tip

In the Service Parameter Configuration window, click Advanced to display this service parameter.

If the parameter specifies true, the Cisco Extension Mobility log in and log out operations using a web proxy are allowed.

If the parameter specifies false, the Cisco Extension Mobility log in and log out requests coming from behind a proxy get rejected.

The setting you select takes effect only if the Validate IP Address parameter specifies true.
Comparing Cisco Extension Mobility Service Parameters

The following table provides a comparison of the Cisco Extension Mobility service parameters and how each service parameter behaves when used to configure the Extension Mobility feature or the Extension Mobility Cross Cluster feature.

### Table 9-3  Comparison of Cisco Extension Mobility Service Parameter Behavior

<table>
<thead>
<tr>
<th>Service Parameter Name</th>
<th>Behavior in Extension Mobility Feature</th>
<th>Behavior in Extension Mobility Cross Cluster Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce Intra-cluster Maximum Login Time</td>
<td>Supported (True or False)</td>
<td>Does not apply. EMCC always enforces auto logout based on the inter-cluster maximum login time.</td>
</tr>
<tr>
<td>Intra-cluster Maximum Login Time</td>
<td>Value gets used if maximum login time is enforced.</td>
<td>Does not apply.</td>
</tr>
<tr>
<td>Inter-cluster Maximum Login Time</td>
<td>Does not apply.</td>
<td>This service parameter shares the same range for Intra-cluster Maximum Login Time, except that it can be set to zero.</td>
</tr>
</tbody>
</table>
### Table 9-3  Comparison of Cisco Extension Mobility Service Parameter Behavior (continued)

<table>
<thead>
<tr>
<th>Service Parameter Name</th>
<th>Behavior in Extension Mobility Feature</th>
<th>Behavior in Extension Mobility Cross Cluster Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Concurrent Requests</td>
<td>Supported. This service parameter combines both EM and EMCC login requests.</td>
<td>Supported. This service parameter combines both EM and EMCC login requests. This service parameter applies only to the home cluster.</td>
</tr>
</tbody>
</table>
| Intra-cluster Multiple Login Behavior | Supported. Values specify the following:  
- Multiple Logins Allowed  
- Multiple Logins Not Allowed  
- Auto Logout | Always allows multiple EMCC logins (Multiple Login Allowed). |
| Alphanumeric User ID | Supported | Supported. Value of visiting cluster gets used. |
| Remember the Last User Logged In | Supported | Supported |
| Clear Call Logs on Intra-Cluster EM | Supported. Values specify the following:  
- True = Clear the call history.  
- False = Do not clear call history after login and logout. | Always get cleared once the phone runs the full cycle reset after login. |
| Validate IP Address | Supported. Validates the IP address of the device during login and logout. | Supported. Validates the IP address in the visiting cluster (vEMApp) during login. Validates the IP address in the home cluster (hEMApp) during logout. |
| Trusted List of IPs | Supported | Supported. Works in conjunction with Validate IP Address parameter. The parameter of home cluster or visiting cluster gets applied, depending on login or logout. |
| Allow Proxy | Supported | Does not apply. |
| EMCC Allow Proxy | Does not apply. | Supported |
| Extension Mobility Cache Size | Supported. Values specify the following:  
- Multiple Logins Allowed  
- Multiple Logins Not Allowed  
- Auto Logout | Supported. Uses the Max Cache Size value in the home cluster. |

**Additional Information**

See the Related Topics, page 9-35.
Creating a Default Device Profile for Each Cisco Unified IP Phone Type

Configure a clusterwide default device profile for each type of Cisco Unified IP Phone that you want to support Cisco Extension Mobility. The phone takes on the default device profile whenever a user logs in to a phone type for which the user has no user device profile.

For more information on how Default Device Profiles work, see the “Overview of Cisco Extension Mobility” section on page 9-6.

To add a default device profile for a phone type, perform the following procedure.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Default Device Profile.

The Default Device Profile Configuration window displays.

Step 2 From the Device Profile Type drop-down list box, choose the device (such as a Cisco 7970) to which a profile gets created.

Step 3 Click Next.

Step 4 If applicable, from the Device Protocol drop-down list box, choose a protocol.

Step 5 Click Next.

Step 6 From the User Hold Audio Source field, choose from the drop-down list box to specify the audio source that plays when a user initiates a hold action.

If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or, if the device pool does not specify an audio source ID, the system default.

Tip You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.

Step 7 At the User Locale drop-down list box, choose the locale that is associated with the phone user interface.

The user locale identifies a set of detailed information, including language and font, to support users. Cisco Unified Communications Manager makes this field available only for phone types that support localization.

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.

Note If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Cisco Unified Communications Operating System Administration Guide.

Step 8 At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the phone buttons on Cisco Unified IP Phones.
Step 9  At the Softkey Template field, choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Choose None if you want to use the softkey profile that is configured in Common Device Configuration.

Step 10  From the Privacy drop-down list box, choose On for each phone that wants Privacy. For more configuration information, see the “Barge and Privacy” section on page 1-1.

Step 11  From the Single Button Barge drop-down list, choose one of the following options:
- **Off**—This device does not allow users to use the Single Button Barge/cBarge feature.
- **Barge**—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge in to a call by using Barge.
- **cBarge**—Choosing this option allows users to press the Single Button cBarge shared-line button on the phone to barge in to a call by using cBarge.
- **Default**—This device inherits the Single Button Barge/cBarge setting from the service parameter.

For more configuration information, see the “Barge and Privacy” section on page 1-1.

Step 12  From the Join Across Lines drop-down list, choose one of the following options:
- **Off**—This device does not allow users to use the Join Across Lines feature.
- **On**—This device allows users to join calls across multiple lines.
- **Default**—This device inherits the Join Across Lines setting from the service parameter.

For more information, see “Understanding Directory Numbers” in the Cisco Unified Communications Manager System Guide.

Step 13  To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the “Ignore Presentation Indicators (internal calls only)” check box.

**Note**  Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern-level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, see the Call Display Restrictions chapter.

Step 14  To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

**Note**  See the “Multilevel Precedence and Preemption” section on page 35-1 for more information.

1. At the MLPP Domain, use the drop-down list box to choose the MLPP domain that is associated with this device profile.

2. If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call.

   From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:
   - **Default**—This device inherits its MLPP indication setting from its device pool.
   - **Off**—This device does not send indication of an MLPP precedence call.
   - **On**—This device does send indication of an MLPP precedence call.
Note: Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

c. If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:

- **Default**—This device inherits its MLPP preemption setting from its device pool.
- **Disabled**—This device does not preempt calls in progress when it places an MLPP precedence call.
- **Forceful**—This device preempts calls in progress when it places an MLPP precedence call.

Note: Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

---

**Step 15**

Click **Save**.

---

**Additional Information**

See the [Related Topics, page 9-35](#).

### Creating the Device Profile for a User

The User Device Profile contains attributes such as name, description, phone template, addon modules, directory numbers, subscribed services, and speed-dial information.

**Note**

Before proceeding, you must ensure that a device profile name and phone button template(s) are configured.

To add a default device profile for a new user of Cisco Extension Mobility, perform the following procedure.

**Note**

If you configure BLF speed-dial buttons in the Device Profile Configuration window, a device that supports Cisco Extension Mobility can display the real-time status of the BLF speed-dial buttons after you log in to the device; that is, if the Presence Group that is applied to the device profile allows you to view the status of the presence entity. See the “Presence” chapter for more details.

**Procedure**

**Step 1**

From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Device Profile**.

The Find and List Device Profiles window displays.
**Step 2**  Click Add New.

The Device Profile Configuration window displays.

From the Device Profile Type drop-down list box, choose the device type and click Next.

If applicable, from the Device Protocol field, choose a protocol.

Click Next.

**Step 3**  At the Device Profile Name field, enter a name of your choice for the device profile. You can make this text anything that describes this particular user device profile, such as “Extension Mobility.”

**Step 4**  At the User Locale drop-down list box, choose the locale that is associated with the phone user interface.

The user locale identifies a set of detailed information, including language and font, to support users. Cisco Unified Communications Manager makes this field available only for phone models that support localization.

> **Note**  If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.

> **Note**  If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the *Cisco Unified Communications Operating System Administration Guide*.

**Step 5**  At the Phone Button Template field, choose the appropriate phone button template. The phone button template determines the configuration of the phone buttons on Cisco Unified IP Phones.

**Step 6**  From the Softkey Template drop-down list box, choose a softkey template. If you want to use the softkey template that is configured in the Common Device Configuration, choose None.

**Step 7**  From the Privacy drop-down list box, choose On for each phone that wants Privacy. For more configuration information, see the “Barge and Privacy” section on page 1-1.

**Step 8**  To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box.

> **Note**  To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box on the Device Profile Configuration window and also on the Phone Configuration window (see the “Subscribing Cisco Unified IP Phones to Cisco Extension Mobility” section on page 9-32).

**Step 9**  If the phone type supports Cisco Unified IP Phone Expansion Modules, Cisco Unified Communications Manager displays expansion module field. At the Module 1 drop-down list box and at the Module 2 drop-down list box, choose the appropriate expansion module.

> **Note**  You may view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate window pops up and displays the phone buttons for that particular expansion module.
Step 10  To configure Multilevel Precedence and Preemption (MLPP) information, perform the following tasks:

\[\text{Note}\]  See the “Multilevel Precedence and Preemption” section on page 35-1 for more information.

a. From the MLPP Domain drop-down list box, choose a hexadecimal value for the MLPP domain that is associated with this device profile.

b. If available, the MLPP Indication setting specifies whether a device will use the capability when it places the MLPP precedence call. From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:
   - **Default**—This device inherits its MLPP indication setting from its device pool.
   - **Off**—This device does not send indication of an MLPP precedence call.
   - **On**—This device does send indication of an MLPP precedence call.

\[\text{Note}\]  Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

c. If available, the MLPP Preemption setting specifies whether a device that is capable of preempting calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting from the following options to assign to devices that use this default device profile:
   - **Default**—This device inherits its MLPP preemption setting from its device pool.
   - **Disabled**—This device does not preempt calls in progress when it places an MLPP precedence call.
   - **Forceful**—This device preempts calls in progress when it places an MLPP precedence call.

\[\text{Note}\]  Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off while MLPP Preemption is set to Forceful.

Step 11  From the Login User Id drop-down list box, choose a user ID. Click **Save**. The page refreshes.

Step 12  From the Association Information section, click the Add a new DN link.  

Step 13  At the Directory Number field, enter the directory number and click **Save**. See “Directory Number Configuration Settings” in the *Cisco Unified Communications Manager Administration Guide* for field descriptions.

Step 14  The following prompt displays: Changes to Line or Directory Number settings require restart. Click **Reset** and follow the prompts.

Step 15  To subscribe the Extension Mobility service to this device profile, go to the Related Links drop-down list box in the upper, right corner of the window and choose Subscribe/Unsubscribe Services; then, click **Go**. A separate Subscribed Cisco IP Phone Services for window displays.
Step 16 From the Select a Service drop-down list box, choose the Extension Mobility service.
Step 17 Click Next.
Step 18 Click Subscribe.
    The new service displays under Subscribed Services.
Step 19 Click Save.
Step 20 To unsubscribe a service, click Unsubscribe and Save.

Additional Information
See the “Device Profile Configuration” chapter in the Cisco Unified Communications Manager Administration Guide for more details of configuring a device profile.

Associating a User Device Profile to a User

You associate a User Device Profile to a user in the same way that you associate a physical device. For more details, see the “Associating Cisco Extension Mobility Profiles” section in the Cisco Unified Communications Manager Administration Guide.

Tip
You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco Extension Mobility at one time. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

To associate a user device profile to a user for Cisco Extension Mobility, follow these steps:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose User Management > End User.
Step 2 Click Add New.
Step 3 Enter the appropriate settings as described in “Changing an End User Password” in the Cisco Unified Communications Manager Administration Guide.
Step 4 To save your changes and add the user, click Save.

Note
To choose an existing end user, click Find and then choose the end user to whom you want to associate a user device profile. See the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Additional Information
See the Related Topics, page 9-35.
**Subscribing Cisco Unified IP Phones to Cisco Extension Mobility**

**Prerequisite**
You must configure the Cisco Unified IP Phones in Cisco Unified Communications Manager before you subscribe the phones to Cisco Extension Mobility. To configure the phones, see the “Cisco Unified IP Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

For a review of device profiles, see the “Understanding Device Profiles” section on page 9-5.

To subscribe to the Cisco Extension Mobility service, perform the following procedure.

**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, choose Device > Phone.

**Step 2**
Click Add New.

**Note**
You can also search and update a configured phone as described in “Phone Configuration Settings” in the Cisco Unified Communications Manager Administration Guide.

The Add a New Phone window displays.

**Step 3**
From the Phone Type drop-down list box, choose the phone type to which you want to subscribe extension mobility and click Next.

**Step 4**
From the Select the device protocol drop-down list box, choose the protocol of the phone and click Next.

**Step 5**
In Extension Information, check the Enable Extension Mobility check box.

**Note**
For descriptions of all fields, see “Configuring Speed-Dial Buttons or Abbreviated Dialing” in the Cisco Unified Communications Manager Administration Guide.

**Step 6**
From the Log Out Profile drop-down list box, choose the profile that you want the phone to use when no extension mobility user is logged in. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed.

**Note**
If you select a specific configured profile, a mapping between the login device and the login profile gets retained after the user logs out. If you select Use Current Device Settings, no mapping gets retained.

The remaining fields show the current device information with regard to the login status of the device: Log in Time, Log out Time.

**Step 7**
On the Cisco Unified Communications Manager Phone Configuration window, to enable the Call Party Restrictions feature, check the Ignore Presentation Indicators check box.

**Note**
To enable the Call Display Restrictions feature, check the Ignore Presentation Indicators (internal calls only) check box on the Phone Configuration window and also on the Device Profile Configuration window (see the “Creating the Device Profile for a User” section on page 9-28). For information about this feature, see the “Call Display Restrictions” chapter.
Step 8  Click Save.
You must now subscribe the extension mobility IP phone service to both the device profile that you
created in the “Creating the Device Profile for a User” section on page 9-28 and to the IP phone target
device.

Step 9  To subscribe extension mobility to the IP phone, go to the Related Links drop-down list box in the upper,
right corner of the window and choose Subscribe/Unsubscribe Services; then, click Go.
A separate Subscribed Cisco IP Phone Services for window displays.

Step 10 From the Select a Service drop-down list box, choose the Extension Mobility service.

Step 11 Click Next.

Step 12 Click Subscribe.
The new service displays under Subscribed Services.

Step 13 Click Save.

Step 14 To unsubscribe a service, click Unsubscribe and Save.

Note To subscribe/unsubscribe services to a device profile, see the “Creating the Device Profile for a
User” section on page 9-28

You have now configured Cisco Extension Mobility.

Additional Information
See the Related Topics, page 9-35.

Configuring the Change Credential IP Phone Service

Configure the Change Credential IP Phone service and associate this phone service with a user, a user
device profile, or a Cisco Unified IP Phone, so that a Cisco Extension Mobility user can change the user
PIN on the Cisco Unified IP Phone to which they have logged in.

The Change Credential IP phone service allows an end user to change the user PIN on the Cisco Unified
IP Phone with both Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster.

Prerequisite
You must configure the Cisco Unified IP Phones in Cisco Unified Communications Manager before you
subscribe the phones to Cisco Extension Mobility. To configure the phones, see the “Cisco Unified IP
Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

For a review of device profiles, see the “Understanding Device Profiles” section on page 9-5.
To add the Change Credential IP Phone service, perform the following procedure.

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Device > Device Settings >
Phone Services.

Step 2  Click Add New.
The IP Phone Services Configuration window displays.

**Step 3**
In the Service Name field, enter Change Credential.

**Note**
For descriptions of all fields, see the “IP Phone Service Configuration Settings” section in the *Cisco Unified Communications Manager Administration Guide*.

**Step 4**
In the Service URL field, enter the following value, where *server* designates the server where the Change Credential IP phone service runs:

```
http://server:8080/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

**Step 5**
In the Secure-Service URL field, enter the following value, where *server* designates the server where the Change Credential IP phone service runs:

```
https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

**Step 6**
Configure the remaining fields in the IP Phone Services Configuration window, and click **Save**.

You must now subscribe the Change Credential IP phone service to both the IP phone target device and to the user device profile that you created in the “Creating the Device Profile for a User” section on page 9-28.

**Step 7**
To subscribe the Cisco Unified IP Phone to the Change Credential IP phone service, display the Phone Configuration window for the phone (**Device > Phone**).

**Step 8**
In the Phone Configuration window, go to the Related Links drop-down list box in the upper, right corner of the window and choose **Subscribe/Unsubscribe Services**; then, click **Go**.

A separate Subscribed Cisco IP Phone Services for window displays.

**Step 9**
From the Select a Service drop-down list box, choose the Change Credential IP phone service.

**Step 10**
Click **Next**.

**Step 11**
Click **Subscribe**.

**Step 12**
The Change Credential IP phone service displays under Subscribed Services.

**Step 13**
Click **Save**.

**Note**
To subscribe/unsubscribe services to a user device profile, see the “Creating the Device Profile for a User” section on page 9-28.

**Note**
To subscribe/unsubscribe services to an end user, see the “End User Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

**Additional Information**
See the Related Topics, page 9-35.
Providing Information to Cisco Extension Mobility Users

After you have configured the system for Cisco Extension Mobility, provide your phone users with the following information:

- Notification of feature availability and the phone types that support Cisco Extension Mobility. Include the name that you gave the Cisco Extension Mobility feature (for example, extension mobility). In addition, notification of changes with respect to activation and deactivation of extension mobility service on any node in the Cisco Unified Communications Manager cluster.
- User password, UserID, and PIN
- URL for the Cisco Unified CM User Options window for the user to change user password and PIN

**Note**
Be aware that user passwords and PINs can only contain characters that the IP phones support: the digits 0 - 9 and their corresponding letters, the asterisk (*), and the octothorpe or pound sign (#).

- Their phone user guide that contains a Cisco Extension Mobility overview and instructions on logging in, logging out, and troubleshooting the feature. The phone user guide also contains information on using Cisco Unified CM User Options window.
- Description of the feature login and logout behavior that you defined in the “Setting the Service Parameters” section on page 9-20.

**Note**
When a user logs in from a phone and the phone displays a “Change PIN” message, the end user must change the end user PIN. When a user logs in from a phone and the phone displays a “Change Password” message, the Cisco Unified Communications Manager administrator must change the CCMSysUser password.

Additional Information
See the Related Topics, page 9-35.

Related Topics

- Configuration Checklist for Cisco Extension Mobility, page 9-1
- Introducing Cisco Extension Mobility, page 9-5
  - Understanding Device Profiles, page 9-5
  - Overview of Cisco Extension Mobility, page 9-6
  - Login and Logout Behavior, page 9-8
  - Login and Logout Behavior, page 9-8
  - Login Call Flow, page 9-9
  - Logout Call Flow, page 9-10
  - Extension Mobility Equivalency, page 9-11
- System Requirements for Cisco Extension Mobility, page 9-13
- Interactions and Restrictions, page 9-14
- Interactions, page 9-14
- Restrictions, page 9-16

- Installing Cisco Extension Mobility for the First Time, page 9-17
- Configuring Cisco Extension Mobility, page 9-17
  - Configuration Guidelines, page 9-17
  - Configuration Example 1, page 9-18
  - Configuration Example 2, page 9-18
  - Adding the Cisco Extension Mobility Service, page 9-19
  - Setting the Service Parameters, page 9-20
  - Comparing Cisco Extension Mobility Service Parameters, page 9-24
  - Creating a Default Device Profile for Each Cisco Unified IP Phone Type, page 9-26
  - Creating the Device Profile for a User, page 9-28
  - Associating a User Device Profile to a User, page 9-31
  - Subscribing Cisco Unified IP Phones to Cisco Extension Mobility, page 9-32
  - Configuring the Change Credential IP Phone Service, page 9-33

- Providing Information to Cisco Extension Mobility Users, page 9-35

Other Configuration
- Internet Protocol Version 6 (IPv6), page 29-1
- Cisco Extension Mobility Cross Cluster, Cisco Unified Communications Manager Features and Services Guide
- Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Default Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- End User Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Finding an Actively Logged-In Device, Cisco Unified Communications Manager Administration Guide
- Intercom Directory Number Configuration, page 28-28

Additional Documentation
The Cisco Extension Mobility Cross Cluster feature allows an enterprise user of one Cisco Unified Communications Manager cluster (the *home cluster*) to log in to a Cisco Unified IP Phone of another Cisco Unified Communications Manager cluster (the *visiting cluster*) during travel as if the user is using the IP phone at the home office.

**Note**

If a user remains in a single cluster, configuration of the Cisco Extension Mobility feature suffices to provide the user with extension mobility capabilities. See the “Cisco Extension Mobility” chapter for a description and configuration details of the Cisco Extension Mobility feature.

This chapter contains the following topics:

- Configuration Checklist for EMCC, page 10-2
- Introducing EMCC, page 10-13
  - EMCC vs. Cisco Extension Mobility, page 10-14
  - EMCC Solution, page 10-14
  - EMCC Login, page 10-15
  - EMCC Supported Phones, page 10-20
  - EMCC Configuration, page 10-21
  - EMCC Active and Remote Login Summary, page 10-21
  - EMCC Call Processing, page 10-22
  - Phone Behavior With EMCC, page 10-33
  - Phone Security With EMCC, page 10-38
- System Requirements for EMCC, page 10-38
- Interactions and Restrictions, page 10-39
  - EMCC Interactions, page 10-39
  - EMCC Restrictions, page 10-40
- Installing and Activating EMCC, page 10-41
- Configuring EMCC, page 10-42
  - Configuring EMCC Feature Configuration Settings, page 10-42
  - EMCC Intercluster Service Profile Configuration Settings, page 10-47
  - Remote Cluster Configuration Settings, page 10-48
Configuration Checklist for EMCC

Table 10-1 provides a checklist for configuring Cisco Extension Mobility Cross Cluster in your network. Use Table 10-1 in conjunction with the “Related Topics” section on page 10-54.

Table 10-1  Cisco Extension Mobility Cross Cluster Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| In Cisco Unified Serviceability, choose **Tools > Service Activation**. Enter a server and activate the following CM Services by checking the check box next to each service name:  
  - Cisco CallManager  
  - Cisco Tftp  
  - Cisco Extension Mobility  
  - Cisco Bulk Provisioning Service (can activate only on the publisher)  
<p>| Click Save, click OK in response to the popup window, and wait for the services to get activated. | See the Cisco Unified Serviceability Administration Guide for additional details. |</p>
<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> Create an Extension Mobility phone service:</td>
<td><strong>IP Phone Services Configuration, Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Device Settings &gt; Phone Services</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Add New</strong>, and fill in the fields in the IP Phone Services Configuration window as follows:</td>
<td></td>
</tr>
<tr>
<td>Service Name: Extension Mobility</td>
<td></td>
</tr>
<tr>
<td>ASCII Service Name: Extension Mobility</td>
<td></td>
</tr>
<tr>
<td>Service Description: Extension Mobility</td>
<td></td>
</tr>
<tr>
<td>Service URL:</td>
<td></td>
</tr>
<tr>
<td><a href="http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#&amp;EMCC=#EMCC#">http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#&amp;EMCC=#EMCC#</a></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Change the IP address in both the Service URL and Secure-Service URL fields, unless you do not want the secure-service URL, in which case you can omit the https:// URL that follows.</td>
<td></td>
</tr>
<tr>
<td>Secure-Service URL:</td>
<td></td>
</tr>
<tr>
<td><a href="https://10.89.80.19:8443/emapp/EMAppServlet?device=#DEVICENAME#&amp;EMCC=#EMCC#">https://10.89.80.19:8443/emapp/EMAppServlet?device=#DEVICENAME#&amp;EMCC=#EMCC#</a></td>
<td></td>
</tr>
<tr>
<td>Check the Enable check box.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> If you click on the Enterprise Subscription check box when configuring the Extension Mobility IP phone service for the first time, you will set up this IP phone service as an enterprise subscription service. If you do this, all phones and device profiles in the enterprise will automatically subscribe to this IP phone service without needing to subscribe individually.</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Save</strong> to save the Extension Mobility phone service.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Checklist for EMCC

#### Table 10-1  Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> Add a device profile for users who need Extension Mobility. The device profile gets used to overlay with a real device when the user logs in (both for Extension Mobility and Extension Mobility Cross Cluster). Follow these steps:</td>
<td></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Device Settings &gt; Device Profile</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Add a new device profile for a specific device type with a specific protocol, assigning a meaningful name to the new device profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong>: 7975 SCCP Device Profile</td>
<td></td>
</tr>
<tr>
<td>3. In the new device profile, configure the Extension Mobility Cross Cluster CSS field.</td>
<td></td>
</tr>
<tr>
<td>This calling search space (CSS) gets applied to the real device configuration when the user travels and uses an IP phone of a different (visiting) cluster.</td>
<td></td>
</tr>
<tr>
<td>Configure this field as if setting the Calling Search Space field in the Phone Configuration window of a local IP phone.</td>
<td></td>
</tr>
<tr>
<td>See the “EMCC Call Routing” section on page 10-27 for more details about the Extension Mobility Cross Cluster CSS field.</td>
<td></td>
</tr>
<tr>
<td>4. Add a directory number (DN) to the new device profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong>: 4001</td>
<td></td>
</tr>
<tr>
<td>5. In the Directory Number Configuration window, choose the Configure Device (&lt;your new device profile name&gt;) option in the Related Links drop-down list box, then click Go.</td>
<td></td>
</tr>
<tr>
<td>You return to the Device Profile Configuration window.</td>
<td></td>
</tr>
<tr>
<td>6. In the Device Profile Configuration window, choose the Subscribe/Unsubscribe Services option in the Related Links drop-down list box, then click Go.</td>
<td></td>
</tr>
<tr>
<td>7. In the popup window that displays, choose the Extension Mobility service in the Select a Service drop-down list box.</td>
<td></td>
</tr>
<tr>
<td>8. Click Next, then click Subscribe.</td>
<td></td>
</tr>
<tr>
<td>9. Click Save and close the popup window.</td>
<td></td>
</tr>
<tr>
<td>10. In the Device Profile Configuration window, click Save.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10-1  Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> Add users for Cisco Extension Mobility Cross Cluster:</td>
<td><strong>End User Configuration, Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose <strong>User Management &gt; End User</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Add New</strong> to add a new end user.</td>
<td></td>
</tr>
<tr>
<td>3. In the End User Configuration window that displays, configure at least the following fields:</td>
<td></td>
</tr>
<tr>
<td>User ID, Password, PIN, Last name, First name</td>
<td></td>
</tr>
<tr>
<td>4. In the Extension Mobility pane, check the Enable Extension Mobility Cross Cluster check box.</td>
<td></td>
</tr>
<tr>
<td>5. Choose the device profile that you configured in <strong>Step 3</strong> from the Available Profiles list pane in the Extension Mobility pane.</td>
<td></td>
</tr>
<tr>
<td>6. Use the Down arrow to move the device profile to the Controlled Profiles list pane.</td>
<td></td>
</tr>
<tr>
<td>7. Click <strong>Save</strong> to save the end user configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Enable Extension Mobility on the devices:</td>
<td><strong>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Phone</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Find the phone on which users can perform Extension Mobility or Extension Mobility Cross Cluster.</td>
<td></td>
</tr>
<tr>
<td>3. For this device, check the Enable Extension Mobility check box in the Extension Information pane.</td>
<td></td>
</tr>
<tr>
<td>4. In the Phone Configuration window, choose the Subscribe/Unsubscribe Services option in the Related Links drop-down list box, then click <strong>Go</strong>.</td>
<td></td>
</tr>
<tr>
<td>5. In the popup window that displays, choose the Extension Mobility service in the Select a Service drop-down list box.</td>
<td></td>
</tr>
<tr>
<td>6. Click <strong>Next</strong>, then click <strong>Subscribe</strong>.</td>
<td></td>
</tr>
<tr>
<td>7. Click <strong>Save</strong> and close the popup window.</td>
<td></td>
</tr>
<tr>
<td>8. In the Phone Configuration window, click <strong>Save</strong>. If indicated, click <strong>OK</strong> in the popup window that displays.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This step completes the configuration necessary for a user to perform intra-cluster extension mobility login.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The Phone Configuration window provides a Secure Services URL. If left blank, the URL Services enterprise parameter gets used.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 10-1 Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>Configure Bulk Certificate Management:</td>
<td>See the “Security” chapter in the <em>Cisco Unified Communications Operating System Administration Guide</em> for details.</td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Operating System Administration, choose <strong>Security &gt; Bulk Certificate Management</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. In the Bulk Certificate Management window that displays, configure the fields as follows:</td>
<td></td>
</tr>
<tr>
<td>IP Address: Specify the IP address of the SFTP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This is the centralized secure FTP server that all participating clusters must share.</td>
<td></td>
</tr>
<tr>
<td>Port: 22 (for SSH default port)</td>
<td></td>
</tr>
<tr>
<td>User ID: User ID of user that has write access</td>
<td></td>
</tr>
<tr>
<td>Password: Password of user that has write access</td>
<td></td>
</tr>
<tr>
<td>Directory: Directory of user that has write access (Example: /tmp)</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Save</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>Configure Bulk Certificate Export:</td>
<td>See the <em>Cisco Unified Communications Operating System Administration Guide</em> for details.</td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Operating System Administration, choose <strong>Security &gt; Bulk Certificate Management</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Click the Export icon.</td>
<td></td>
</tr>
<tr>
<td>3. In the Bulk Certificate Export window that displays, configure the following field:</td>
<td></td>
</tr>
<tr>
<td>Certificate Type: All</td>
<td></td>
</tr>
<tr>
<td>4. Click <strong>Export</strong>, then click <strong>Close</strong>.</td>
<td></td>
</tr>
<tr>
<td>This step creates a PKCS12 file that contains certificates for all nodes in the cluster.</td>
<td></td>
</tr>
<tr>
<td>Every participating cluster must export certificates to the same SFTP server and SFTP directory.</td>
<td></td>
</tr>
<tr>
<td>A cluster must export its certificates whenever the Tomcat or TFTP certificate(s) gets regenerated on any of its nodes.</td>
<td></td>
</tr>
</tbody>
</table>
## Step 8: Consolidate Certificates

Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters have exported their certificates to the SFTP server.

1. In Cisco Unified Communications Operating System Administration, choose **Security > Bulk Certificate Management > Consolidate > Bulk Certificate Consolidate**.

   Consolidate certificates when all participating clusters have exported their certificates.

2. In the window that displays, configure the following field:
   - Certificate Type: All

3. Click **Consolidate**.

   This step consolidates all PKCS12 files in the SFTP server to form a single file.

   Only one of the participating clusters needs to perform consolidation.

   If new certificates are exported after they are consolidated, consolidation needs to be performed again to pick up the newly exported certificates.

### Related Procedures and Topics

See the *Cisco Unified Communications Operating System Administration Guide* for details.

## Step 9: Import Certificates

This step imports the consolidated PKCS12 file from the SFTP server into the local cluster.

1. In Cisco Unified Communications Operating System Administration, choose **Security > Bulk Certificate Management > Import > Bulk Certificate Import**.

2. In the window that displays, configure the following field:
   - Certificate Type: All

3. Click **Import**.

   After you import all the certificates on each cluster, for each cluster, you need to restart Cisco CallManager service and Cisco Tomcat service to activate the services for each node on each cluster.

   After an upgrade, these certificates are preserved. Users do not need to reimport or reconsolidate certificates.

   This step imports the consolidated PKCS12 file from the SFTP server into the local cluster.

   All clusters should re-import when any participating cluster makes an export.

   Perform import after a central administrator consolidates the certificates as explained in **Step 8**.

### Related Procedures and Topics

See the *Cisco Unified Communications Operating System Administration Guide* for details.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>Consolidate certificates:</td>
<td></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Operating System Administration, choose <strong>Security &gt; Bulk Certificate Management &gt; Consolidate &gt; Bulk Certificate Consolidate</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters have exported their certificates to the SFTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Certificate Type: All</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Consolidate</strong></td>
</tr>
<tr>
<td></td>
<td>This step consolidates all PKCS12 files in the SFTP server to form a single file.</td>
</tr>
<tr>
<td></td>
<td>Only one of the participating clusters needs to perform consolidation.</td>
</tr>
<tr>
<td></td>
<td>If new certificates are exported after they are consolidated, consolidation needs to be performed again to pick up the newly exported certificates.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>Import certificates:</td>
<td></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Operating System Administration, choose <strong>Security &gt; Bulk Certificate Management &gt; Import &gt; Bulk Certificate Import</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. In the window that displays, configure the following field:</td>
<td></td>
</tr>
<tr>
<td>Certificate Type: All</td>
<td></td>
</tr>
<tr>
<td>3. Click <strong>Import</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>After you import all the certificates on each cluster, for each cluster, you need to restart Cisco CallManager service and Cisco Tomcat service to activate the services for each node on each cluster.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>After an upgrade, these certificates are preserved. Users do not need to reimport or reconsolidate certificates.</td>
</tr>
<tr>
<td></td>
<td>This step imports the consolidated PKCS12 file from the SFTP server into the local cluster.</td>
</tr>
<tr>
<td></td>
<td>All clusters should re-import when any participating cluster makes an export.</td>
</tr>
<tr>
<td></td>
<td>Perform import after a central administrator consolidates the certificates as explained in <strong>Step 8</strong>.</td>
</tr>
</tbody>
</table>
Table 10-1    Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>To enable EMCC for video calls, configure Common Phone Profile (Device &gt; Device Settings &gt; Common Phone Profile) or configure Enterprise Phone Configuration (System &gt; Enterprise Phone Configuration) to enable video calls. In either window, set the Video Capabilities drop-down list box as Enabled. (This setting may be enabled by default per cluster.)</td>
<td>Common Phone Profile Configuration, Cisco Unified Communications Manager Administration Guide Enterprise Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>Add EMCC devices—Add EMCC Templates:</td>
<td>See the Cisco Unified Communications Manager Bulk Administration Guide for details.</td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose Bulk Administration &gt; EMCC &gt; EMCC Template.</td>
<td></td>
</tr>
<tr>
<td>2. Click Add New.</td>
<td></td>
</tr>
<tr>
<td>3. In the EMCC Template Configuration window, configure the fields as follows:</td>
<td></td>
</tr>
<tr>
<td>Template Name: EMCC Device Template</td>
<td></td>
</tr>
<tr>
<td>Device Pool: Default</td>
<td></td>
</tr>
<tr>
<td>SIP Profile: Standard SIP Profile</td>
<td></td>
</tr>
<tr>
<td>Common Device Configuration: Default Common Device Configuration</td>
<td></td>
</tr>
<tr>
<td>4. Click Save.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>Add EMCC devices—Set default EMCC template.</td>
<td>See the Cisco Unified Communications Manager Bulk Administration Guide for details.</td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose Bulk Administration &gt; EMCC &gt; Insert/Update EMCC.</td>
<td></td>
</tr>
<tr>
<td>2. Click Update EMCC Devices.</td>
<td></td>
</tr>
<tr>
<td>3. In the Default EMCC Template drop-down list box, choose the EMCC Device Template that you configured in Step 11.</td>
<td></td>
</tr>
<tr>
<td>4. Click Run Immediately.</td>
<td></td>
</tr>
<tr>
<td>5. Click Submit.</td>
<td></td>
</tr>
<tr>
<td>6. Verify whether the job ran successfully:</td>
<td></td>
</tr>
<tr>
<td>Choose Bulk Administration &gt; Job Scheduler and look for the Job ID of your job. Check that your job ran successfully.</td>
<td></td>
</tr>
</tbody>
</table>
Step 13  Add EMCC devices—Insert the EMCC Devices:

1. In Cisco Unified Communications Manager Administration, choose Bulk Administration > EMCC > Insert/Update EMCC.
2. Click Insert EMCC Devices.
3. Change the value in the Number of EMCC Devices to be added field (for example, to 5).
4. Click Run Immediately and click Submit.
5. Refresh this window and check that the Number of EMCC Devices already in database value now displays the number of devices that you added (for example, 5).
6. Alternately, choose Bulk Administration > Job Scheduler to check on whether the job completed successfully.

Maximum Number of EMCC Base Devices To Add
Include EMCC in the total number of devices that get supported in the cluster, using the following calculation:

phones + (2 x EMCC devices) <= MaxPhones

Cisco Unified Communications Manager systems specify a MaxPhones value of 60,000.
EMCC login does not affect the number of licenses that get used in the home cluster.

Step 14  Configure enterprise parameters and add a geolocation filter:

1. In Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters.
2. For the Cluster ID enterprise parameter, configure a unique cluster ID for every participating cluster.
3. In Cisco Unified Communications Manager Administration, choose System > Geolocation Filter.
4. Click Add New.
5. Create a new geolocation filter.
   Example name: EMCC Geolocation Filter.
   Specify criteria for matching, such as Country, State, and City.

See the Cisco Unified Communications Manager Bulk Administration Guide for details.
Chapter 10 Cisco Extension Mobility Cross Cluster

Table 10-1 Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 15</strong> Configure EMCC feature parameters:</td>
<td>Configuring EMCC Feature Configuration Settings, page 10-42</td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose Advanced Features &gt; EMCC &gt; EMCC Feature Configuration.</td>
<td></td>
</tr>
<tr>
<td>2. In the EMCC Feature Configuration window that displays, configure the following feature parameters:</td>
<td></td>
</tr>
<tr>
<td>Default TFTP Server for EMCC Login Device</td>
<td></td>
</tr>
<tr>
<td>EMCC Geolocation Filter</td>
<td></td>
</tr>
<tr>
<td>Default Server for Remote Cluster Update</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Each feature parameter must be previously configured before you can choose them in the drop-down list box that associates with each feature parameter.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> You can keep the default values for other EMCC feature parameters or you can change as needed.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10-1  Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| **Step 16**  
  Configure one or two intercluster SIP trunks for EMCC.  
  **Note**  
  You may configure one trunk for both PSTN Access and RSVP Agent services (in **Step 17**) or one trunk for each service. You need no more than two EMCC SIP trunks.  
  1. In Cisco Unified Communications Manager Administration, choose **Device > Trunk**.  
  2. Click **Add New**.  
  3. Specify the following settings:  
     Trunk Type: SIP Trunk  
     Trunk Service Type: Extension Mobility Cross Clusters  
  4. Click **Next**.  
  5. In the Trunk Configuration window that displays, specify the following settings in the Device Information pane. The following values show example values.  
     Name: EMCC-ICT-SIP-Trunk-1  
     Device Pool: Default  
     In the SIP Information pane, specify the following example settings:  
     SIP Trunk Security Profile: Non Secure SIP Trunk Profile  
     SIP Profile: Standard SIP Profile  
     In the Geolocation Configuration pane, specify the following setting:  
     Send Geolocation Information: Check this check box.  
  **Note**  
  EMCC trunk must specify SendGeolocation as True, MTPRequired as False, and UnattendedPort as False.  
  6. Click **Save** to save the intercluster SIP trunk for EMCC.  

**Trunk Configuration, Cisco Unified Communications Manager Administration Guide**
### Step 17: Configure EMCC intercluster service profile:

1. In Cisco Unified Communications Manager Administration, choose **Advance Features > EMCC > EMCC Intercluster Service Profile**.
2. Check the **Active** check box in the EMCC pane.
3. Check the **Active** check box in the PSTN Access pane.
4. In the PSTN Access SIP Trunk drop-down list box, choose a SIP trunk that you configured in **Step 16**.
5. Check the **Active** check box in the RSVP Agent pane.
6. In the RSVP Agent SIP Trunk drop-down list box, choose another SIP trunk that you configured in **Step 16**.

**Note**

If you configured only one trunk in **Step 16**, you can choose the same trunk for RSVP Agent SIP Trunk as for PSTN Access SIP Trunk.

7. Click **Validate** to validate your settings.
8. If no failure messages display in the popup window, click **Save**.

### Step 18: Configure EMCC remote cluster services:

1. In Cisco Unified Communications Manager Administration, choose **Advance Features > EMCC > EMCC Remote Cluster**.
2. Click **Add New**.
3. In the Remote Cluster Configuration window that displays, configure the following settings:
   - Cluster ID: Ensure that this cluster ID matches the enterprise parameter value of the cluster ID of the other cluster(s).
   - Fully Qualified Name: Use the IP address of the remote cluster or a domain name that can resolve to any node on the remote cluster.

**Related Procedures and Topics**

- EMCC Intercluster Service Profile Configuration Settings, page 10-47
- Remote Cluster Configuration Settings, page 10-48
Chapter 10    Cisco Extension Mobility Cross Cluster

Introducing EMCC

This section contains information on the following topics:

- EMCC vs. Cisco Extension Mobility, page 10-14
- EMCC Solution, page 10-14
- EMCC Login, page 10-15
- EMCC Supported Phones, page 10-20
- EMCC Configuration, page 10-21
- EMCC Active and Remote Login Summary, page 10-21
- EMCC Call Processing, page 10-22
- Phone Behavior With EMCC, page 10-33
- Phone Security With EMCC, page 10-38

---

Table 10-1    Cisco Extension Mobility Cross Cluster Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 19</strong></td>
<td></td>
</tr>
<tr>
<td>Configure service parameters:</td>
<td></td>
</tr>
<tr>
<td>1. In Cisco Unified Communications Manager Administration, choose <strong>System &gt; Service Parameters</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. From the Server drop-down list box, choose a server.</td>
<td></td>
</tr>
<tr>
<td>3. From the Service drop-down list box, choose the Cisco Extension Mobility service.</td>
<td></td>
</tr>
<tr>
<td>4. Click the <strong>Advanced</strong> button at the top of the window.</td>
<td></td>
</tr>
<tr>
<td>5. As needed, configure the following service parameters in the Clusterwide Parameters (Parameters that apply to all servers) pane:</td>
<td></td>
</tr>
<tr>
<td>- Inter-cluster Maximum Login Time</td>
<td></td>
</tr>
<tr>
<td>- EMCC Allow Proxy: Set this value as <strong>True</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> For EMCC, the call logs always get cleared.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> For EMCC, multiple logins are always allowed.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 20**        |                             |
| EMCC does not require any special configuration for SRST to function. |                             |
| If SRST configuration is required for your system, configure as usual. |                             |

| **Service Parameter Configuration**, Cisco Unified Communications Manager Administration Guide |
| Setting the Service Parameters, page 9-20 |
| Comparing Cisco Extension Mobility Service Parameters, page 9-24 |

---

Survivable Remote Site Telephony Configuration, Cisco Unified Communications Manager Administration Guide
EMCC vs. Cisco Extension Mobility

Release 3.1 of Cisco CallManager first offered the Cisco Extension Mobility feature. Cisco Extension Mobility continues to apply only to intra-cluster users and devices. Customers, however, want a seamless experience, no matter where they log in:

- User wants the same set of features and services: all lines, speed dials, message button, MWI, and features.
- Administrator wants security, CAC, local gateway access, local media resources, and serviceability.

EMCC Challenges

With intra-cluster Cisco Extension Mobility, the following characteristics apply:

- Device information is available in the local database.
- User information is available in the local database.
- Global information is available in the local database.

With inter-cluster Cisco Extension Mobility, the following characteristics apply:

- Device information is in one cluster database.
- User information is in another cluster database.
- Global information, such as routing configuration and service parameters, is in the database of both clusters.

Cisco Extension Mobility presents the following challenge: either device information needs to be moved to the cluster that manages user information or vice-versa.

EMCC Solution

The solution to address the problem of extension mobility across clusters specifies cross-registration. Cross-registration implies the following characteristics:

- User from home cluster logs in to a phone at visiting cluster.
- Login procedure conveys the device information into the home cluster database.
- Home cluster database builds a temporary device with user device profile.
- Home cluster TFTP server builds the phone configuration file.
- After login, visiting cluster directs the phone to home cluster TFTP server.
- Phone downloads its TFTP configuration from home cluster (HC) TFTP server and then cross-registers with home cluster Cisco Unified Communications Manager.

Note

Clusters are designated as home or visiting relative to the login user.

Cisco Extension Mobility Cross Cluster Interactions

See the “EMCC Interactions” section on page 10-39 for a list of the interactions between the Cisco Extension Mobility Cross Cluster feature and other features.
Scope of EMCC
Cisco Extension Mobility Cross Cluster supports the following features:

- Cisco Extension Mobility login and logout
  - User authentication takes place across clusters.
- Security
  - Cross-cluster security gets provided by default.
  - Cisco Unified IP Phones with nonsecure security profiles get supported.
- PSTN access is suitable for the visiting phone.
  - Routing E911 to the right part of the PSTN (that is, to local gateways) takes place.
  - Routing local calls to the right part of the PSTN takes place.
  - Calls terminating to local route groups route to local gateways in the visiting cluster.
- Media resources suitable for the visiting phone get presented, such as the following:
  - RSVP Agent, TRP, Music On Hold (MOH), MTP, transcoder, conference bridge
- Call Admission Control (CAC)
  - Home cluster remains ignorant of visiting cluster locations and regions.
  - The system cannot apply Cisco Unified Communications Manager locations and regions across the cluster boundaries.
- RSVP agent-based CAC using RSVP agents in the visiting cluster
- Call features and services that home cluster can reasonably support
  - Example restriction: Intercom configuration specifies configuration to a static device, so Cisco Extension Mobility Cross Cluster does not support the Intercom feature.
- Default max audio bit-rate for EMCC login device is set to 8 kbps (G.729).

Note
If home cluster uses software conference bridge that supports only the G.711 codec and if no transcoder is configured in the visiting cluster, conference will fail. As a workaround, change the EMCC feature parameter, EMCC Region Max Audio Bit Rate, to 64 kbps (G.711).

EMCC Login
This section presents the following topics:

- EMCC Login Terminology, page 10-15
- EMCC Login Progress, page 10-17

EMCC Login Terminology

Figure 10-1 illustrates the visiting cluster versus a home cluster in Cisco Extension Mobility Cross Cluster.
Introducing EMCC

Visiting Cluster
For the visiting cluster, the following characteristics apply:
- Phone is geographically present here.
- Phone configuration resides here in the visiting Cisco Unified Communications Manager database.
- The resources that the phone needs reside here, such as gateways and RSVP agents.
- The visiting phone normally registers with the visiting Cisco Unified Communications Manager cluster that manages this geographic location (prior to EMCC login).
- CCMCIP specifies the Cisco CallManager Cisco IP Phone service.

Home Cluster
For the home cluster, the following characteristics apply:
- End user configuration resides here.
- User device profile (lines, speed dials, features, and many more user characteristics) reside here.
- User dialing habits make sense in the home context.
- User locale resides here.

Cross-registration specifies the process of importing the device data into the home cluster and building a device record that is combined with the end user Extension Mobility (EM) profile in the home cluster, then directing the phone to register directly with the home cluster Cisco Unified Communications Manager.
EMCC Login Progress

Figure 10-2 illustrates Cisco Extension Mobility Cross Cluster login when extension mobility finds the home cluster.

**Figure 10-2  EMCC Login—Extension Mobility Finds Home Cluster**
Figure 10-3 illustrates Cisco Extension Mobility Cross Cluster login when extension mobility authenticates, gives information to home cluster, and prepares home cluster.

Figure 10-3  EMCC Login—Extension Mobility Authenticates, Gives Information to Home, Prepares Home
Figure 10-4 illustrates Cisco Extension Mobility Cross Cluster login when extension mobility modifies the visiting cluster and initiates reregistration.

Mini-config specifies a small configuration file built by the visiting cluster to redirect the phone to the home cluster after login.
Figure 10-5 illustrates Cisco Extension Mobility Cross Cluster login when extension mobility login services complete processing and the phone reregisters.

**Figure 10-5 EMCC Login—Extension Mobility Login Services Complete Processing and the Phone Reregisters**

**EMCC Supported Phones**

The list of devices that support the Cisco Extension Mobility Cross Cluster varies per version and device pack.

Use the Cisco Unified Reporting application to generate a complete list of devices that support Cisco Extension Mobility Cross Cluster for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click System Reports in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all devices that support Cisco Extension Mobility Cross Cluster, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Extension Mobility Cross Cluster

   The List Features pane displays a list of all devices that support the Cisco Extension Mobility Cross Cluster feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

   For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*, which you can find at this URL:

### EMCC Configuration

See the “**Configuration Checklist for EMCC**” section on page 10-2 for an overview of the configuration steps to configure Cisco Extension Mobility Cross Cluster, both in Cisco Unified Communications Manager Administration and in the other Cisco Unified Communications components, such as Cisco Unified Serviceability and the Cisco Unified Communications Operating System.

For details of configuring menu options that apply exclusively to EMCC, see the “**Configuring EMCC**” section on page 10-42 and its subsections.

### EMCC Active and Remote Login Summary

In the user home cluster, the administrator can view a list of the cluster users who have logged in from remote devices.

To do so, the administrator performs the following steps:

1. In Cisco Unified Communications Manager Administration, execute **Device > Phone**.
   - The Find and List Phones window displays.

2. From the Related Links drop-down list box, choose Remotely Logged In Device, then click **Go**.

For additional information about the remotely logged-in devices report, see the “**Finding a Remotely Logged-In Device**” section in the *Cisco Unified Communications Manager Administration Guide*.

In any cluster, the administrator can view a list of the cluster devices that have been logged in to either Cisco Extension Mobility or Cisco Extension Mobility Cross Cluster.

To do so, the administrator performs the following steps:

1. In Cisco Unified Communications Manager Administration, execute **Device > Phone**.
   - The Find and List Phones window displays.

2. From the Related Links drop-down list box, choose Actively Logged In Device Report, then click **Go**.

For additional information about the actively logged-in devices report, see the “**Finding an Actively Logged-In Device**” section in the *Cisco Unified Communications Manager Administration Guide*.
EMCC Call Processing

This section presents the following topics:

- EMCC Call Processing Overview, page 10-23
- EMCC Call-Processing Characteristics, page 10-23
- EMCC Call-Processing Requirements, page 10-24
- EMCC Call-Processing for Emergency Calls, page 10-24
- Finding the Roaming Device Pool, page 10-24
- EMCC Call-Processing Configuration, page 10-25
- List EMCC Phones and Their Roaming Device Pools in Home Cluster, page 10-26
- EMCC Call Processing in Home Cluster, page 10-26
- EMCC Call Routing, page 10-27
- Configuring Visiting Cluster Emergency Pattern in Home Cluster, page 10-27
- Local Route Group Routing of EMCC Visiting Phone in Home Cluster, page 10-28
- Local Route Group Routing Using EMCC SIP Trunk, page 10-28
- EMCC Calling Search Space in Device Profile, page 10-29
- Region Configuration for EMCC Phones, page 10-29
- RSVP Configuration for EMCC Phones, page 10-29
- RSVP Agent-Based CAC Basic Call, page 10-30
- RSVP Agent CAC Hold/Resume by Home Phone, page 10-31
- RSVP Agent CAC Hold/Resume by Visiting Phone, page 10-32
- EMCC Common Call-Processing Issues, page 10-32
- Obtaining Help for EMCC Call-Processing Issues, page 10-33
EMCC Call Processing Overview

Figure 10-6 provides an overview of EMCC call processing.

Figure 10-6  EMCC Call Processing

EMCC Call-Processing Characteristics

EMCC call processing exhibits the following characteristics:

- Call control on the home cluster
  - Visiting phone registers with home cluster.
- RSVP Agent gets allocated from visiting cluster but is indirectly controlled by home cluster.
  - Visiting phone registers with home cluster.
  - Follows home cluster policy for RSVP-based CAC.
- Codec selection by both home cluster and visiting cluster
  - Media processes on both home cluster and visiting cluster.
  - Codec selected based on EMCC region configuration of both clusters
- Emergency call routing is visiting phone/visiting cluster dependent.
  - Home cluster supports both home cluster and visiting cluster emergency pattern.
  - Route emergency calls back to visiting cluster with local route group via EMCC SIP intercluster trunk.
  - Uses local route group of visiting phone that is configured in visiting cluster.
- Device-dependent PSTN access in visiting cluster
  - Route call from SIP trunk to local gateway colocated with visiting phone
EMCC Call-Processing Requirements

Cisco Extension Mobility Cross Cluster fulfills the following call-processing requirements:

- Emergency call routing
  - Allows user to dial either home cluster emergency pattern or visiting cluster emergency pattern (for example, 999 in the United Kingdom or 911 in the United States).
  - Call must route to the local gateway in the visiting cluster no matter which cluster emergency pattern gets dialed.
- RSVP agent based CAC
  - RSVP Agents in the visiting cluster must get allocated based on the visiting phone media resource group list (MRGL) in the visiting cluster.

Note: Whereas the phone registers with the home cluster, moving the phone location in the visiting cluster may cause incorrect association to the local gateway or media resource group list (MRGL) in the visiting cluster.

EMCC Call-Processing for Emergency Calls

Figure 10-7 illustrates Cisco Extension Mobility Cross Cluster call processing for emergency calls.

Finding the Roaming Device Pool

Finding the roaming device pool exhibits the following characteristics:

- EMCC phone finds roaming-sensitive attributes from its roaming device pool in home cluster.
• Home cluster configures one roaming device pool per remote cluster, with distinct geolocation characterizing that cluster, for example:
  - DPforUKCluster (country=UK)
  - DPforSJCluster (country=US, A1=CA, A3=SJ)
• Phone that is enabled for extension mobility in visiting cluster configures its geolocation in visiting cluster.
• Login process sends phone geolocation from visiting cluster to home cluster.
• EMCC geolocation filter that is configured in home cluster filters phone geolocation.
• Home cluster uses filtered phone geolocation to find the most suitable device pool as phone roaming device pool while phone registers in home cluster.

Matching the Roaming Device Pool By Using Geolocation in Home Cluster

Figure 10-8 illustrates matching the roaming device pool by using the geolocation in the home cluster.

EMCC Call-Processing Configuration

Visiting cluster configures geolocation for phones that are enabled for extension mobility. This configuration takes place in the Geolocation field of the Phone Configuration window (Device > Phone) or in the Geolocation field of the Geolocation Configuration pane of the Device Pool Configuration window (System > Device Pool).
Introducing EMCC

Configuration of the following entities is also required for extension mobility enabled phones in the visiting cluster:

- Local route group in the associated Device Pool Configuration window (System > Device Pool)
- RSVP device (transcoder or MTP) in the phone media resource group list if RSVP policy is enabled.

Home cluster configures EMCC geolocation filter. Use the Advanced Features > EMCC > EMCC Feature Configuration menu option to configure the EMCC Geolocation Filter setting.

One device pool per remote cluster serves as the roaming device pool for login phones.

Example

Device pool specifies **EMCC Device Pool for UK Cluster**.

Geolocation for this device pool specifies **UK Geolocation**.

The UK Geolocation geolocation in this device pool allows UK phones to match and choose this device pool as the roaming device pool when the phones log in.

List EMCC Phones and Their Roaming Device Pools in Home Cluster

The home cluster administrator can list all remote devices that are currently registered to this cluster. To do so, execute **Device > Phone**. From the Related Links drop-down list box, choose Remotely Logged In Device; then, click **Go**.

The Remotely Logged-In Device Report displays the following information:

- Device Name
- Logged In Profile
- User ID
- Remote Cluster ID
- Roaming Device Pool

EMCC Call Processing in Home Cluster

Logged-in EMCC phones in home cluster acquire the following attributes and preferences:

- Shared attributes from EMCC base device (Bulk Administration)
- Roaming-sensitive attributes from its roaming device pool
  - One roaming device pool per remote cluster
  - EMCC phones of same visiting cluster choose the same roaming DP
  - Allows country-specific emergency dialing plan (for example, 999 for UK)
- User preferences from User Device Profile (lines and speed dials)
- Feature-specific attributes from EMCC Feature Configuration
  - Codec preference for all EMCC phone of all clusters
  - RSVP policy for EMCC phones
EMCC Call Routing

Call routing gets based on calling search space (CSS) home cluster builds for the phone.

Home cluster concatenates the CSS in the following priority order:

1. Adjunct CSS (new)
   - Configured in roaming device pool to support country-specific emergency dialing plan (for example, UK phone remotely registers back to US cluster; user dials 9.999 (UK emergency number) that US cluster will normally not recognize. Home cluster=US, visiting cluster=UK.
   - May skip Adjunct CSS configuration if home cluster and visiting cluster share the same emergency pattern.

2. Line CSS

3. Device CSS
   - Device-specific; gets configured in Phone Configuration window or its static device pool.
   - Allows phone to perform normal dialing in home cluster.
   - Visiting phone does not have phone device configured in home cluster.
   - Home cluster takes EMCC CSS (new) from user login device profile and uses this CSS as its static device CSS.

Adjunct Calling Search Space Functionality

To configure the adjunct CSS, execute System > Device Pool and configure the Adjunct CSS field in the Device Pool Settings pane.

In this example, the following configuration applies:

- Adjunct CSS specifies Adjunct CSS for UK Cluster.
- Selected Partitions (in Route Partitions for this Calling Search Space) specifies EMCC Emergency Partition for UK.

The adjunct CSS, which you configure in the device pool, enables UK emergency dialing from UK phone that registers to US cluster after login and binding to the roaming device pool. US cluster specifies the home cluster.

Calling search space specifies only one member partition, EMCC Emergency Partition for UK.

Configuring Visiting Cluster Emergency Pattern in Home Cluster

Configure a visiting cluster emergency pattern in the home cluster.

Example

Configure the route for 9.999/{EMCC emergency partition for UK}. This route contain only one member, Standard LRG.

If visiting phone (in UK) that registers to home cluster (in US) dials 9.999, this pattern matches route pattern 9.999/{EMCC emergency partition for UK} because of the adjunct CSS in the phone roaming device pool. As a result, home cluster (US cluster) routes the call to the device local route group.
Local Route Group Routing of EMCC Visiting Phone in Home Cluster

The local route group of EMCC visiting phone in the home cluster specifies the following:

- Local route group of a device comprises gateways to the device local PSTN.
- Calls that terminate to Standard LRG get directed to calling device LRG (that is, to gateways that connect to the local PSTN).
- A normal phone and its local route group register to the same cluster.
- EMCC visiting phone and its local route group register to different clusters.
  - Home cluster has no configured local route group of visiting phone.
  - Home cluster has no direct access to local PSTN gateways of visiting phone.
  - Calls that terminate to Standard LRG of EMCC visiting phone in home cluster get directed to visiting cluster via PSTN access SIP trunk (EMCC Configuration).
  - Visiting cluster finds local route group that is configured for visiting phone. (Remember that any phone that is enabled for extension mobility must configure its local route group in the visiting cluster.)
  - Visiting cluster routes the call to gateways in that local route group like a normal phone.

Local Route Group Routing Using EMCC SIP Trunk

Figure 10-9 illustrates local route group routing that uses an EMCC SIP trunk.

Figure 10-9  Local Route Group Routing Using EMCC SIP Trunk

- User dials 9999.
- VC may override the CSS of EMCC SIP Trunk with calling phone CSS (Advanced Features > EMCC > EMCC Configuration > CSS for PSTN Access SIP Trunk).
- MMm ... This device is an EMCC device from UK cluster, I am going to route this call to UK cluster via the configured EMCC SIP Trunk for PSTN Access (Advanced Features > EMCC > Intercluster Service Profile).
- This device has Adjunct CSS with partition (EMCC emergency partition for UK)
  - I can match the RP: 9.999/(EMCC emergency partition for UK) with route resolved to Standard LRG.
- DA indicates that 999 call should route to Standard LRG. Because this is EMCC SIP Trunk, I will use calling device LRG, not SIP Trunk LRG, to route the call.
EMCC Calling Search Space in Device Profile

The Extension Mobility Cross Cluster CSS field, which you define in the Device Profile Configuration window (Device > Device Settings > Device Profile), gets used as the device CSS of the remote phone when the user selects this device profile during EMCC login.

Region Configuration for EMCC Phones

Region configuration for EMCC phones specifies the following:

- EMCC login phones do not have region configured in home cluster.
- All EMCC login phones, from any cluster, are assigned with common region configuration (Advanced Features > EMCC > EMCC Feature Configuration) that overrides normal region configuration.
- EMCC feature parameters for regions must get configured with identical values in all clusters. If EMCC feature parameters for regions are set with different values, the Remote Cluster Update operation disables RSVP Agent for the cluster in question.
- The following EMCC feature parameters for regions apply:
  - EMCC Region Max Audio Bit Rate (See the “Scope of EMCC” section on page 10-15 for a details of a suggested workaround configuration that involves this feature parameter.)
  - EMCC Region Max Video Call Bit Rate (includes Audio)
  - EMCC Region Link Loss Type

RSVP Configuration for EMCC Phones

RSVP configuration for EMCC phones presents the following characteristics:

- In home cluster, RSVP policy for EMCC phones follow the same configuration steps as normal phones:
  - Configure a common location (for example, Remote-cluster-location) or cluster-specific location (for example, UK-location).
  - Set Unlimited audio and video bandwidth for the location(s) such that location-based CAC gets disabled.
  - Set RSVP policy for location pairs (no reservation, optional, mandatory).
- In visiting cluster, add RSVP devices to the media resource group list (MRGL) of the visiting phone.
- When allocating RSVP agent, home cluster Cisco Unified Communications Manager recognizes the RSVP agent is for EMCC phone and redirects the request to visiting cluster over RSVP SIP trunk.
- When allocating all other media resources, home cluster Cisco Unified Communications Manager allocate media resources based on the media resource group list that is configured in the home cluster.
RSVP Agent-Based CAC Basic Call

Figure 10-10 illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Call Admission Control (CAC) basic call.

Figure 10-10  EMCC for RSVP Agent-Based CAC Basic Call
RSVP Agent CAC Hold/Resume by Home Phone

Figure 10-11 illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Hold/Resume call by the home phone.

**Figure 10-11** EMCC for an RSVP Agent-Based CAC Hold/Resume Call by the Home Phone
RSVP Agent CAC Hold/Resume by Visiting Phone

Figure 10-12 illustrates Cisco Extension Mobility Cross Cluster for an RSVP Agent-based Hold/Resume call by the visiting phone.

Figure 10-12 EMCC for an RSVP Agent-Based CAC Hold/Resume Call by the Visiting Phone

EMCC Common Call-Processing Issues

This section discusses the following common call processing issues that EMCC can present:

- Cannot make normal call.
  - EMCC phone does not bind to the correct roaming device pool (Device > Phone, then choose Remotely Logged In Device).
  - Login device profile does not set EMCC CSS (Device > Device Setting > Device Profile).
  - RSVP reservation fails if configured (for example, no RSVP device in visiting phone media resource group list in visiting cluster).
  - EMCC login phone does not support G.729 codec and no transcoder is configured for the phone in the visiting cluster.

- Cannot make emergency call.
  - EMCC phone does not bind to the correct roaming device pool (Device > Phone, then choose Remotely Logged In Device).
  - Adjunct CSS in roaming device pool of EMCC phone is missing.
  - Verify routing configuration in home cluster based on Adjunct CSS.
  - Local route group configuration is missing in phone static device pool in visiting cluster.
Introducing EMCC

- No media or one-way media is present.
  - Check whether all clusters have the same value in EMCC Region configuration window (Advanced Features > EMCC > EMCC Feature Configuration).
  - Check RSVP policy in home cluster (only RSVP policy in home cluster matters).

Obtaining Help for EMCC Call-Processing Issues

Take the following steps to obtain help for call processing issues:
- Collect detailed traces from both home cluster and visiting cluster.
- Provide detailed description of the call scenario:
  - Identify the EMCC device and the non-EMCC device and its cluster. For example, the EMCC phone does not bind to the correct roaming device pool. Use the Device > Phone menu option, then choose Remotely Logged In Device from the Related Links drop-down list box.

Phone Behavior With EMCC

This section presents the following phone behaviors in an EMCC environment:
- WAN Network Failure—Configuration File Unavailable, page 10-34
- EMCC Failure—Registration Rejection, page 10-35
- EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Interoffice Failure, page 10-36
- EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure, page 10-37
- EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure (No Visiting SRST), page 10-38
WAN Network Failure— Configuration File Unavailable

Figure 10-13 illustrates WAN network failure when the configuration file is unavailable.

The phone reregisters with the visiting cluster.

In EMCC login mode, if the phone detects a connection failure to the home cluster, the phone tries to reestablish connection to the home cluster. After several failed attempts, such as failures due to WAN failure, the phone issues a logout request to the visiting cluster automatically, then the phone reregisters with the visiting cluster as logged out.
EMCC Failure—Registration Rejection

Figure 10-14 illustrates EMCC failure when registration rejection occurs. The phone reregisters with the visiting cluster.

![Diagram showing EMCC failure—registration rejection](image-url)
EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Interoffice Failure

Figure 10-15 illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable and an interoffice failure occurs.

The phone fails over to SRST.

Figure 10-15  EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Interoffice Failure

Visiting Phone

Visiting SRST

Visiting Unified CM Cluster

Visiting CM Database

Visiting EM

Home Unified CM Cluster

Home CM Database

Home TFTP

Connectivity Check

All Visiting Unified Mobile Communicators Unavailable

Visiting TFTP

2

1

Visiting cluster load

Phone configuration in Visiting vCCM list, AltTFTP= hTFTP, SRST=vSRST

Home cluster load

Phone configuration in Home with user settings hCCM list, AltTFTP=hTFTP, SRST=vSRST
EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure

Figure 10-16 illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable and an inter-cluster failure occurs.

The phone reregisters with the visiting cluster.

Figure 10-16 EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure

- Phone configuration in Visiting (Original configuration)
- Home cluster load
- Phone configuration in Home with user settings hCCM list, AltTFTP=hTFTP, SRST=vSRST
EMCC Failure—Home Cisco Unified Communications Manager Unavailable/Inter-cluster Failure (No Visiting SRST)

Figure 10-17 illustrates EMCC failure when the home Cisco Unified Communications Manager is unavailable, an inter-cluster failure occurs, and no visiting SRST applies. The phone reregisters with the visiting cluster.

Phone Security With EMCC

See the Cisco Unified Communications Manager Security Guide for details of phone security issues in an EMCC environment.

System Requirements for EMCC

The following system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager, Release 8.0(1) or higher
- Cisco Extension Mobility service
- Cisco Unified Communications Operating System
- Cisco Bulk Provisioning service
Other call-control entities that support and use the Cisco Extension Mobility Cross Cluster configuration; for example, other Cisco Unified Communications Manager clusters, EMCC intercluster service profiles, and EMCC remote cluster services

Interactions and Restrictions

This section provides the details of interactions and restrictions for Cisco Extension Mobility Cross Cluster. See the following topics:

- EMCC Interactions, page 10-39
- EMCC Restrictions, page 10-40

EMCC Interactions

This section lists the interactions of the Cisco Extension Mobility Cross Cluster with other Cisco Unified Communications Manager Administration components.

With the Cisco Extension Mobility Cross Cluster cross-registration solution, user features function as expected across clusters. The following list specifies some of the user features that function across clusters:

- Shared lines
- Hunt lists
- Transfer/Conference/Hold
- Call Forward
- Cisco Unified Mobility
- Barge/cBarge
- iDivert
- Applications
- Speed dials
- Services
- Address book
- Device labels
- Line appearance management
- MWI
- Voice mail
- Do Not Disturb
- Monitoring and Recording
- Callback Busy/NR
- Multilevel Precedence and Preemption (MLPP)
EMCC Restrictions

This section lists the restrictions and limitations of the Cisco Extension Mobility Cross Cluster with other Cisco Unified Communications Manager Administration components. The section covers the following topics:

- EMCC Logout Limitation, page 10-40
- EMCC Does Not Support Intercom Feature, page 10-40
- EMCC Does Not Support Location-based Call Admission Control, page 10-40
- EMCC Limitations and Configuration Requirements With Local Route Groups, page 10-40
- EMCC Duplicate User ID Limitation, page 10-40
- EMCC Device Cannot Be Provisioned in More Than One Cluster, page 10-40
- EMCC and Security Mode Among Clusters, page 10-41
- Visiting Phone Login Limitation After Cisco CallManager Service Goes Down, page 10-41
- EMCC and Product-Specific Configuration Layout in Phone Configuration Window, page 10-41

**EMCC Logout Limitation**

If the home cluster administrator disables the EMCC capability of an end user while the end user is logged in with EMCC, the system does not automatically log this end user out. (In this scenario, the administrator unchecks the Enable Extension Mobility Cross Cluster check box in the End User Configuration window for the end user.) Instead, the system only fails future EMCC attempts by this end user. The current EMCC session continues until the end user logs out.

**EMCC Does Not Support Intercom Feature**

Intercom configuration specifies configuration to a static device, so Cisco Extension Mobility Cross Cluster does not support the Intercom feature.

**EMCC Does Not Support Location-based Call Admission Control**

Location CAC does not get supported. RSVP-based CAC does get supported.

**EMCC Limitations and Configuration Requirements With Local Route Groups**

See the following sections for details of EMCC limitations and configuration requirements in routing EMCC calls with local route groups:

- EMCC Call-Processing Configuration, page 10-25
- Configuring Visiting Cluster Emergency Pattern in Home Cluster, page 10-27
- Local Route Group Routing of EMCC Visiting Phone in Home Cluster, page 10-28
- Local Route Group Routing Using EMCC SIP Trunk, page 10-28

**EMCC Duplicate User ID Limitation**

Duplicate user ID does not get supported (for either the same or different PIN), because the behavior is unpredictable.

**EMCC Device Cannot Be Provisioned in More Than One Cluster**

Cisco Systems recommends that autoregistration be disabled (to avoid accidental provisioning).
EMCC and Security Mode Among Clusters

All clusters must specify the same security mode; either
- All clusters specify nonsecure clusters or mixed-mode clusters.
- Clusters with different security modes cannot be mixed.
- Phones that allow Cisco Extension Mobility Cross Cluster must be non-secure mode (that is, they must associate with a nonsecure Device Security Profile).
  - RTP streams only
  - Calls not secure (TCP only, no TLS connection)

Visiting Phone Login Limitation After Cisco CallManager Service Goes Down

The Cisco Extension Mobility service in participating clusters performs a periodic remote cluster update. The EMCC Feature Configuration feature parameter, Remote Cluster Update Interval, controls the update interval, for which the default value specifies 30 minutes.

If the Cisco Extension Mobility service on cluster A does not get back a reply from a remote cluster (such as cluster B) for this update, the Remote Cluster window for cluster A shows that Remote Activated service is set to false for cluster B.

In this case, the visiting cluster does not receive any response from the home cluster and sets the Remote Activated values for the home cluster as false.

During this interval, a visiting phone may not be able to log in by using EMCC. The visiting phone receives the Login is unavailable (23) message.

At this point, trying to log in EMCC from a visiting phone may fail with the error, Login is unavailable (23), which displays on the phone. This occurs because the visiting cluster has not yet detected the change of home cluster Cisco Unified Communications Manager from out-of-service to in-service.

Detection of status change of remote clusters is based on the value of the Remote Cluster Update Interval EMCC feature parameter and on when the visiting Cisco Extension Mobility service performed the last query/update.

You can also click the Update Remote Cluster Now button on the Remote cluster Service Configuration window (Advanced Features > EMCC > EMCC Remote Cluster) to change Remote Activate values to true, which also allows EMCC logins. Otherwise, after the next periodic update cycle, EMCC logins by visiting phones will return to normal.

EMCC and Product-Specific Configuration Layout in Phone Configuration Window

When a user uses a phone in a visiting cluster to log into the user Extension Mobility profile, the phone inherits the default provisioning, network, and security settings (specifically, the configuration in the Product Specific Configuration Layout section of the Phone Configuration window) from the home cluster. This behavior may override local security and network settings that are in place in the visiting cluster. Some of the parameters have firmware defaults that the system administrator cannot change until a fix is provided.

Installing and Activating EMCC

After you install Cisco Unified Communications Manager, your network can support the Cisco Extension Mobility Cross Cluster feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for EMCC” section on page 10-2.
Chapter 10  Cisco Extension Mobility Cross Cluster

Configuring EMCC

This section contains information on the following topics:

- Configuring EMCC Feature Configuration Settings, page 10-42
- EMCC Intercluster Service Profile Configuration Settings, page 10-47
- Remote Cluster Configuration Settings, page 10-48

Configuring EMCC Feature Configuration Settings

Table 10-2 provides detailed descriptions of the EMCC feature parameters that you configure in the EMCC Feature Configuration window (Advanced Features > EMCC > EMCC Feature Configuration).

Table 10-2  EMCC Feature Parameter Configuration Settings

<table>
<thead>
<tr>
<th>EMCC Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default TFTP Server for EMCC Login Device</td>
<td>Choose the computer name or IP address of the default TFTP server that devices logging into EMCC from a remote cluster should use.</td>
</tr>
<tr>
<td>Backup TFTP Server for EMCC Login Device</td>
<td>Choose the computer name or IP address of the backup TFTP server that devices logging into EMCC from a remote cluster should use.</td>
</tr>
<tr>
<td>Default Interval for Expired EMCC Device Maintenance</td>
<td>Specify the number of minutes that elapse between checks of the system for expired EMCC devices. An expired EMCC device specifies a device that logged in to EMCC from a remote cluster, but that, due to WAN failure or a connectivity issue, the phone logged out of the visiting cluster and, when connectivity was restored, logged back into the visiting cluster. During this maintenance job, the Cisco Extension Mobility service checks the Cisco Unified Communications Manager database for any expired EMCC devices and automatically logs such devices out. Default value specifies 1440 minutes. Valid values range from 10 minutes to 1440 minutes.</td>
</tr>
</tbody>
</table>
Table 10-2  EMCC Feature Parameter Configuration Settings (continued)

<table>
<thead>
<tr>
<th>EMCC Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable All Remote Cluster Services When Adding A New Remote Cluster</td>
<td>Choose whether you want all services on a new remote cluster to be automatically enabled when you add a new cluster. Valid values specify True (enable all services on the remote cluster automatically) or False (manually enable the services on the remote cluster via the Remote Cluster Configuration window in Cisco Unified Communications Manager Administration). You may prefer to enable the services manually so that you have time to configure the EMCC feature completely before enabling the remote services. Default value specifies False.</td>
</tr>
<tr>
<td>CSS for PSTN Access SIP Trunk</td>
<td>Choose the calling search space (CSS) that the PSTN Access SIP trunk for processing EMCC calls uses. The PSTN Access SIP trunk specifies the SIP trunk that has been configured for PSTN access in the Intercluster Service Profile window in Cisco Unified Communications Manager Administration. Calls over this trunk are intended for and only get routed to the local PSTN that is co-located with the EMCC logged-in phone that initiates the call. Valid values specify the following:  • Use Trunk CSS (PSTN calls use the local route group, which can prove useful for properly routing emergency service calls)  • Use phone's original device CSS (PSTN calls get routed using the configured calling search space on the remote phone; that is, the CSS that is used when the phone is not logged into EMCC). Default value specifies Use trunk CSS.</td>
</tr>
<tr>
<td>EMCC Geolocation Filter</td>
<td>Choose the geolocation filter that you have configured for use with the Cisco Extension Mobility Cross Cluster feature. You must previously configure the EMCC geolocation filters to be able to choose a value in this drop-down list box. Based on the information in the geolocation that associates with a phone that is logged in via extension mobility from another cluster as well as the selected EMCC geolocation filter, Cisco Unified Communications Manager places the phone into a roaming device pool. Cisco Unified Communications Manager determines which roaming device pool to use by evaluating which device pool best matches the phone geolocation information after the EMCC geolocation filter gets applied.</td>
</tr>
</tbody>
</table>
### Table 10-2 EMCC Feature Parameter Configuration Settings (continued)

<table>
<thead>
<tr>
<th>EMCC Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMCC Region Max Audio Bit Rate</td>
<td>This parameter specifies the maximum audio bit rate for all EMCC calls, regardless of the region associated with the other party.</td>
</tr>
<tr>
<td></td>
<td>Default value specifies 8 kbps (G.729).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Communicate your EMCC Region Max Audio Bit Rate to the other clusters with which your cluster interacts. All participating EMCC clusters must specify the same EMCC Region Max Audio Bit Rate.</td>
</tr>
<tr>
<td>EMCC Region Max Video Call Bit Rate (Includes Audio)</td>
<td>This parameter specifies the maximum video call bit rate for all EMCC video calls, regardless of the maximum video call bit rate of the region associated with the other party.</td>
</tr>
<tr>
<td></td>
<td>Default value specifies 384. Valid values range from 0 to 8128.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Communicate your EMCC Region Max Video Call Bit Rate to the other clusters with which your cluster interacts. All participating EMCC clusters must specify the same EMCC Region Max Video Call Bit Rate.</td>
</tr>
</tbody>
</table>
EMCC Region Link Loss Type

This parameter specifies the link loss type between any EMCC phone and devices in any remote cluster.

**Note** Communicate your EMCC Region Link Loss Type to the other clusters with which your cluster interacts. To allow two-way audio on EMCC calls, all participating EMCC clusters must use the same EMCC Region Link Loss Type.

Based on the option chosen, Cisco Unified Communications Manager attempts to use the optimal audio codec for the EMCC call while observing the configured EMCC Region Max Audio Bit Rate.

Valid values specify the following:

- Lossy (a link where some packet loss can or may occur, for example, DSL)
- Low Loss (a link where low packet loss occurs, for example, T1).

When this parameter is set to Lossy, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality, given the assumption that some packet loss will occur.

When this parameter is set to Low Loss, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality, given the assumption that little or no packet loss will occur.

The only difference in the audio codec preference ordering between the Low Loss and Lossy options is that G.722 is preferred over iSAC (Internet Speech Audio Codec) when the Link Loss Type is set as Low Loss, whereas iSAC is preferred over G.722 when the Link Loss Type is set as Lossy.

Default value specifies Low Loss.
RSVP SIP Trunk KeepAlive Timer
Specify the number of seconds that Cisco Unified Communications Manager waits between sending or receiving KeepAlive messages or acknowledgments between two clusters over EMCC RSVP SIP trunks.
An EMCC RSVP SIP trunk specifies a SIP trunk that has Cisco Extension Mobility Cross Cluster configured as the Trunk Service Type and that has been selected as the SIP Trunk for RSVP Agent in the Intercluster Service Profile window. When two of these intervals elapse without receipt of a KeepAlive message or an acknowledgment, Cisco Unified Communications Manager releases the RSVP resources with the remote cluster.
Default value specifies 15 seconds. Valid values range from 1 second to 600 seconds.

Default Server For Remote Cluster Update
Choose the default server name or IP address of the primary Cisco Unified Communications Manager server in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this server to get information about this local cluster.

Backup Server for Remote Cluster Update
Choose the default server name or IP address of the secondary Cisco Unified Communications Manager server in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this server when the primary server is down to get information about this local cluster.

Remote Cluster Update Interval
Specify an interval, in minutes, during which the Cisco Extension Mobility service on the local Cisco Unified Communications Manager node collects information about the remote EMCC cluster. Collected information includes such details as the remote cluster Cisco Unified Communications Manager version and service information.
Default value specifies 30. Valid values range from 15 minutes to 10,080 minutes.

Additional Information
See the “Related Topics” section on page 10-54.
EMCC Intercluster Service Profile Configuration Settings

In the Intercluster Service Profile Configuration window, you configure an EMCC intercluster service profile. In Cisco Unified Communications Manager Administration, use the Advanced Features > EMCC > EMCC Intercluster Service Profile menu option to display this window.

Table 10-3  EMCC Intercluster Service Profile Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMCC</td>
<td>Check this check box to activate the Cisco Extension Mobility Cross Cluster feature.</td>
</tr>
<tr>
<td>Active</td>
<td>Check this box to activate PSTN access.</td>
</tr>
<tr>
<td>PSTN Access</td>
<td>From the drop-down list box, choose the SIP trunk to use for PSTN access.</td>
</tr>
<tr>
<td></td>
<td>You must first specify a SIP trunk (Device &gt; Trunk) and configure it for PSTN access</td>
</tr>
<tr>
<td>RSVP Agent</td>
<td>Click this box to activate RSVP Agent.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose the SIP trunk to use for RSVP Agent.</td>
</tr>
<tr>
<td></td>
<td>You must first specify a SIP trunk (Device &gt; Trunk).</td>
</tr>
<tr>
<td>EMCC Setup Validation Report</td>
<td>After you click Save, this pane displays the EMCC Setup Validation Report.</td>
</tr>
<tr>
<td></td>
<td>If you click Validate, a popup window, displays the EMCC Setup Validation Report. Click Close to close the popup window.</td>
</tr>
<tr>
<td></td>
<td>The Configuration(s) column of the report displays the following entities that get validated:</td>
</tr>
<tr>
<td></td>
<td>• EMCC PSTN Access Service</td>
</tr>
<tr>
<td></td>
<td>• Default TFTP Server for EMCC Login Device</td>
</tr>
<tr>
<td></td>
<td>• EMCC Geolocation Filter</td>
</tr>
<tr>
<td></td>
<td>• EMCC Service Default Server for Remote Cluster</td>
</tr>
<tr>
<td></td>
<td>• EMCC Devices</td>
</tr>
<tr>
<td></td>
<td>• ClusterId</td>
</tr>
</tbody>
</table>
Configuring EMCC

Additional Information
See the “Related Topics” section on page 10-54.

Remote Cluster Configuration Settings

In Cisco Unified Communications Manager Administration, use the Advanced Features > EMCC > EMCC Remote Cluster menu path to configure remote clusters.

Tips About Finding Remote Clusters
The Find operation locates only those remote clusters that you added previously. The Find operation does not locate the clusters that belong to the enterprise automatically.

Using the GUI
For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table
Table 10-4 provides detailed descriptions of the remote cluster configuration settings that you configure in the Remote Cluster Configuration window (Advanced Features > EMCC > EMCC Remote Cluster).

Table 10-4 Remote Cluster Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Cluster Information</td>
<td></td>
</tr>
<tr>
<td>Cluster Id</td>
<td>Enter the cluster ID of the remote cluster. Valid values include alphanumeric characters, period (.), and hyphen (-).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the remote cluster. This field accepts up to 128 characters. You may use all characters except quotes (&quot;), close angle bracket (*/), open angle bracket (&lt;), backslash (), dash (-), ampersand (&amp;), and percent sign (%).</td>
</tr>
</tbody>
</table>
### Remote Cluster Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Qualified Name</td>
<td>Enter the fully qualified name of the remote cluster. This field accepts up to 50 characters and allows the following characters: alphanumeric (a through z, A through Z, and 0 through 9), period (.), dash (-), asterisk (*), and space ( ).</td>
</tr>
</tbody>
</table>

#### Remote Cluster Service Information

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMCC</td>
<td>For the EMCC service, the following column headings detail the configuration for this service:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—If the EMCC service is enabled, this box gets checked.</td>
</tr>
<tr>
<td></td>
<td>• Service—This entry specifies the EMCC service.</td>
</tr>
<tr>
<td></td>
<td>• Remote Activated—Valid values specify true or false.</td>
</tr>
<tr>
<td></td>
<td>• Address 1—This column lists the first address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 2—This column lists the second address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 3—This column lists the third address for this service.</td>
</tr>
<tr>
<td>PSTN Access</td>
<td>For PSTN access, the following column headings detail the configuration for this service:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—If PSTN access is enabled, this box gets checked.</td>
</tr>
<tr>
<td></td>
<td>• Service—This entry specifies PSTN access.</td>
</tr>
<tr>
<td></td>
<td>• Remote Activated—Valid values specify true or false.</td>
</tr>
<tr>
<td></td>
<td>• Address 1—This column lists the first address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 2—This column lists the second address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 3—This column lists the third address for this service.</td>
</tr>
<tr>
<td>RSVP Agent</td>
<td>For the RSVP Agent, the following column headings detail the configuration for this service:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—If RSVP Agent is enabled, this box gets checked.</td>
</tr>
<tr>
<td></td>
<td>• Service—This entry specifies RSVP Agent.</td>
</tr>
<tr>
<td></td>
<td>• Remote Activated—Valid values specify true or false.</td>
</tr>
<tr>
<td></td>
<td>• Address 1—This column lists the first address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 2—This column lists the second address for this service.</td>
</tr>
<tr>
<td></td>
<td>• Address 3—This column lists the third address for this service.</td>
</tr>
</tbody>
</table>

| Enabled All Services | Click this button to enable all services (EMCC, PSTN Access, and RSVP Agent). |
| Disabled All Services | Click this button to disable all services (EMCC, PSTN Access, and RSVP Agent). |
| Update Remote Cluster Now | Click this button to update the remote cluster immediately. |
Providing Information to End Users

End users log in and out of Extension Mobility Cross Cluster feature just as they do from the Extension Mobility feature, and they receive no indication of which cluster they are using.

Additional Information
See the “Related Topics” section on page 10-54.

Troubleshooting EMCC

This section presents the following topics:
- Error Codes for the Cisco Extension Mobility Application (EMApp), page 10-50
- Error Codes for the Cisco Extension Mobility Service (EMService), page 10-51

Error Codes for the Cisco Extension Mobility Application (EMApp)

Table 10-5 lists and describes the error codes that apply to the Cisco Extension Mobility application (EMApp).

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Please try to login again (201)</td>
<td>Authentication Error</td>
<td>If the user is an EMCC user, this error can occur if “EMCC” is not activated in the Inter-cluster Service Profile page.</td>
</tr>
<tr>
<td>202</td>
<td>Please try to login again (202)</td>
<td>Black userid or pin</td>
<td>User enters blank user ID or PIN.</td>
</tr>
<tr>
<td>204</td>
<td>Login is unavailable (204)</td>
<td>Directory server error</td>
<td>EMAp sends this error to phone when IMS could not authenticate the user with the given PIN.</td>
</tr>
<tr>
<td>205</td>
<td>Login is unavailable (205)</td>
<td>User Profile Absent</td>
<td>Occurs when the user profile information could not be retrieved either from the cache or from the database.</td>
</tr>
<tr>
<td></td>
<td>Logout is unavailable (205)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>207</td>
<td>Login is unavailable(207)</td>
<td>Device Name Empty</td>
<td>Occurs when device or name tag is missing in the request URI. This cannot happen with real devices and can occur only if request is sent from third-party applications.</td>
</tr>
<tr>
<td></td>
<td>Logout is unavailable(207)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 10-5  Error Codes for the Cisco Extension Mobility Application (EMApp) (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>208</td>
<td>Login is unavailable(208) Logout is unavailable(208)</td>
<td>EMService Connection Error</td>
<td>Visiting EMApp could not connect to any Visiting EMService. (Service is down or not activated.) Visiting EMService could not connect to Home EMService (WAN is down or certificates are not trusted.)</td>
</tr>
<tr>
<td>210</td>
<td>Login is unavailable(210) Logout is unavailable(210)</td>
<td>Init Fail-Contact Admin</td>
<td>Some error (like database connection failure) occurred while initializing EMApp. The error may occur because of failure in connecting to the database during startup. This represents a catastrophic error.</td>
</tr>
<tr>
<td>211</td>
<td>Login is unavailable(211) Logout is unavailable(211)</td>
<td>EMCC Not Activated</td>
<td>Occurs when PSTN is not activated in the Intercluster Service Profile window of the visiting cluster.</td>
</tr>
<tr>
<td>212</td>
<td>Login is unavailable(212)</td>
<td>Cluster ID is invalid</td>
<td>Occurs when a remote cluster updated (keep-alive) fails by sending an incorrect cluster ID to remote cluster.</td>
</tr>
<tr>
<td>213</td>
<td>Login is unavailable(213) Logout is unavailable(213)</td>
<td>Device does not support EMCC</td>
<td>Occurs when a device (phone load) does not have EMCC capability (for example, for legacy phones or for TNP phones with older phone load).</td>
</tr>
</tbody>
</table>

Table 10-6  Error Codes for the Cisco Extension Mobility Service (EMService)

Table 10-6 lists and describes the error codes that apply to the Cisco Extension Mobility service (EMService).

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Login is unavailable(0) Logout is unavailable(0)</td>
<td>Unknown Error</td>
<td>EMService failed in some totally unexpected scenario. It is catastrophic.</td>
</tr>
<tr>
<td>1</td>
<td>Login is unavailable(1) Logout is unavailable(1)</td>
<td>Error on parsing</td>
<td>When EMService could not parse the XML request from EMApp/EMService. This happens when 3rd party applications sends an incorrect query/login XML (EM API) or it can occur because of mis-match in version between home and visiting CUCM versions (for EMCC).</td>
</tr>
<tr>
<td>2</td>
<td>Login is unavailable(2)</td>
<td>EMCC Authentication Error</td>
<td>EMCC user credentials could not be authenticated as the user has entered wrong pin.</td>
</tr>
</tbody>
</table>
### Table 10-6  Error Codes for the Cisco Extension Mobility Service (EMSservice) (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Login is unavailable(3) Logout is unavailable(3)</td>
<td>Invalid App User</td>
<td>Invalid application user. This can be seen commonly when using EM API.</td>
</tr>
<tr>
<td>4</td>
<td>Login is unavailable(4) Logout is unavailable(4)</td>
<td>Policy Validation error</td>
<td>EM Service sends this error when it could not validate the login/logout request due to some unknown reason (Error while querying the database or error while retrieving info from cache).</td>
</tr>
<tr>
<td>5</td>
<td>Login is unavailable(5) Logout is unavailable(5)</td>
<td>Dev. logon disabled</td>
<td>EM / EMCC Login is requested for a device which has “Enable extension mobility” unchecked in phone configuration page.</td>
</tr>
<tr>
<td>6</td>
<td>Login is unavailable(6) Logout is unavailable(6)</td>
<td>Database Error</td>
<td>Whenever database throws an exception while executing the query or stored procedure requested by EM Service (login/logout or device/user query), EM Service sends this error code to EM App.</td>
</tr>
<tr>
<td>8</td>
<td>Login is unavailable(8) Logout is unavailable(8)</td>
<td>Query type undetermined</td>
<td>No Valid query has been sent to the EMService (DeviceUserQuery &amp; UserDeviceQuery are valid ones). This is ideally seen when using EM API with incorrect XML input.</td>
</tr>
<tr>
<td>9</td>
<td>Login is unavailable(9) Logout is unavailable(9)</td>
<td>Dir. User Info Error</td>
<td>This error is displayed in two cases:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. IMS throws an exception when it tries to authenticate a particular user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. When information about a particular user could not be retrieved either from cache or database.</td>
</tr>
<tr>
<td>10</td>
<td>Login is unavailable(10) Logout is unavailable(10)</td>
<td>User lacks app proxy rights</td>
<td>User tries to do login/query on behalf of some other user (By default, only CCMSysUser has the admin rights.)</td>
</tr>
<tr>
<td>11</td>
<td>Login is unavailable(11) Logout is unavailable(11)</td>
<td>Device Does not exist</td>
<td>Phone record entry is absent in the device table.</td>
</tr>
<tr>
<td>12</td>
<td>Phone record entry is absent in the device table</td>
<td>Dev. Profile not found</td>
<td>No Device profile is associated with the remote user (EMCC Login)</td>
</tr>
<tr>
<td>18</td>
<td>Login is unavailable(18)</td>
<td>Another user logged in</td>
<td>Another user is already logged in on that particular phone</td>
</tr>
<tr>
<td>19</td>
<td>Log out is unavailable(19)</td>
<td>No user logged in</td>
<td>Trying to logout a user which has not logged in. This can ideally happen when sending logout requests from the 3rd party applications (EM API).</td>
</tr>
<tr>
<td>20</td>
<td>Login is unavailable(20) Logout is unavailable(20)</td>
<td>Hoteling flag error</td>
<td>“Enable extension mobility” is unchecked in phone configuration page.</td>
</tr>
</tbody>
</table>
Table 10-6 Error Codes for the Cisco Extension Mobility Service (EMService) (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Login is unavailable(21) Logout is unavailable(21)</td>
<td>Hoteling Status error</td>
<td>Current user status could not be retrieved from either local cache or database (when PolicyValidator tried to check current login User or login time).</td>
</tr>
<tr>
<td>22</td>
<td>Login is unavailable(22)</td>
<td>Dev. logon disabled</td>
<td>Occurs when EM is not enabled on device and the request is sent via EM API or when the services button is pressed on phone.</td>
</tr>
<tr>
<td>23</td>
<td>Login is Unavailable (23) Logout is Unavailable (23)</td>
<td>User does not exist</td>
<td>Occurs when the given user ID is not found (in any of the remote clusters).</td>
</tr>
<tr>
<td>25</td>
<td>Login is unavailable(25)</td>
<td>User logged in elsewhere</td>
<td>User has currently logged in on some other phone</td>
</tr>
<tr>
<td>26</td>
<td>Login is unavailable(26) Logout is unavailable(26)</td>
<td>Busy, please try again</td>
<td>When EMService has currently reached the threshold level of “Maximum Concurrent Requests” service parameter</td>
</tr>
<tr>
<td>28</td>
<td>Login is unavailable(28) Logout is unavailable(28)</td>
<td>Untrusted IP Error</td>
<td>When “Validate IP Address” service parameter is set to true and user tries to login/logout from a machine whose IP address is not trusted (for example, 3rd party app / EM API from a machine which is not listed in Trusted List of Ips service parameter).</td>
</tr>
<tr>
<td>29</td>
<td>Login is unavailable(29) Logout is unavailable(29)</td>
<td>ris down-contact admin</td>
<td>RISDC Cache has not been created and initialized and EMService is unable to connect to RISDC</td>
</tr>
<tr>
<td>30</td>
<td>Login is unavailable(30) Logout is unavailable(30)</td>
<td>Proxy not allowed</td>
<td>When login/logout comes through proxy (“Via” is set in HTTP header) and “Allow Proxy” service parameter is set to “false.”</td>
</tr>
<tr>
<td>31</td>
<td>Login is unavailable(31) Logout is unavailable(31)</td>
<td>EMCC Not Activated for the user</td>
<td>Occurs when Enable Extension Mobility Cross Cluster check box is not checked in the End User window of the home cluster.</td>
</tr>
<tr>
<td>32</td>
<td>Login is unavailable(32) Logout is unavailable(32)</td>
<td>Device does not support EMCC</td>
<td>Occurs when a device model does not have EMCC capability (for example, legacy phones)</td>
</tr>
<tr>
<td>33</td>
<td>Login is unavailable(33) Logout is unavailable(33)</td>
<td>No free EMCC dummy device</td>
<td>Occurs when all the EMCC dummy devices are in use by other EMCC logins.</td>
</tr>
<tr>
<td>35</td>
<td>Login is unavailable(35) Logout is unavailable(35)</td>
<td>Visiting Cluster Information is not present in Home Cluster</td>
<td>Occurs when the home cluster does not have an entry for this visiting cluster.</td>
</tr>
<tr>
<td>36</td>
<td>Login is unavailable(36) Logout is unavailable(36)</td>
<td>No Remote Cluster</td>
<td>Occurs when the administrator has not added any remote cluster.</td>
</tr>
<tr>
<td>37</td>
<td>Login is Unavailable (37) Logout is Unavailable (37)</td>
<td>Duplicate Device Name</td>
<td>Occurs when the same device name exists in both home cluster and visiting cluster.</td>
</tr>
</tbody>
</table>
Table 10-6  Error Codes for the Cisco Extension Mobility Service (EMService) (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Phone Display</th>
<th>Quick Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Login is unavailable(38) Logout is unavailable(38)</td>
<td>EMCC Not Allowed</td>
<td>Occurs when home cluster does not want to allow EMCC login (Enable Extension Mobility Cross Cluster check box is not checked in the home cluster).</td>
</tr>
<tr>
<td>42</td>
<td>Login is unavailable(42) Logout is unavailable(42)</td>
<td>Invalid ClusterID</td>
<td>Occurs when the remote cluster ID is not valid (happens during remote cluster update)</td>
</tr>
<tr>
<td>43</td>
<td>Login is unavailable(43)</td>
<td>Device Security mode error</td>
<td>Device Security Profile associated to the EMCC device should be Non Secure for its Device Security Mode.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuration Checklist for EMCC, page 10-2
- Introducing EMCC, page 10-13
  - EMCC vs. Cisco Extension Mobility, page 10-14
  - EMCC Solution, page 10-14
  - EMCC Login, page 10-15
  - EMCC Supported Phones, page 10-20
  - EMCC Configuration, page 10-21
  - EMCC Active and Remote Login Summary, page 10-21
  - EMCC Call Processing, page 10-22
  - Phone Behavior With EMCC, page 10-33
  - Phone Security With EMCC, page 10-38
- System Requirements for EMCC, page 10-38
- Interactions and Restrictions, page 10-39
  - EMCC Interactions, page 10-39
  - EMCC Restrictions, page 10-40
- Installing and Activating EMCC, page 10-41
- Configuring EMCC, page 10-42
  - Configuring EMCC Feature Configuration Settings, page 10-42
  - EMCC Intercluster Service Profile Configuration Settings, page 10-47
  - Remote Cluster Configuration Settings, page 10-48
- Providing Information to End Users, page 10-50
- Troubleshooting EMCC, page 10-50
  - Error Codes for the Cisco Extension Mobility Application (EMApp), page 10-50
  - Error Codes for the Cisco Extension Mobility Service (EMService), page 10-51
Other Configuration

- Cisco Extension Mobility, *Cisco Unified Communications Manager Features and Services Guide*
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*
- Device Profile Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*

Additional Documentation

Cisco Unified Communications Manager Assistant With Proxy Line Support

The Cisco Unified Communications Manager Assistant feature enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support. The Cisco IP Manager Assistant service supports both proxy line and shared line support simultaneously in a cluster. For information about Cisco Unified Communications Manager Assistant with shared line support, see the “Cisco Unified Communications Manager Assistant With Shared Line Support” section on page 12-1.

Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants. To accommodate this number of users, the administrator configures up to three Cisco Unified Communications Manager Assistant applications in one Cisco Unified Communications Manager cluster and assigns managers and assistants to each instance of the application.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager and the assistant, and assistant console interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified Communications Manager Assistant users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

This chapter provides the following information about Cisco Unified Communications Manager Assistant:

- Configuration Checklist for Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-2
- Introducing Cisco Unified Communications Manager Assistant, page 11-5
- System Requirements for Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-12
- Interactions and Restrictions, page 11-13
- Installing and Activating Cisco Unified Communications Manager Assistant, page 11-17
- Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-18
- Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants, page 11-41
Configuration Checklist for Cisco Unified Communications Manager Assistant with Proxy Line Support

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. When you configure Cisco Unified Communications Manager Assistant in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but an alternate number chosen by the system that an assistant uses to handle manager calls. In proxy-line mode, a manager and an assistant have access to all features that are available in Cisco Unified Communications Manager Assistant, which include default assistant selection, assistant watch, call filtering, and divert all calls.

Table 11-1 lists the steps for configuring Cisco Unified Communications Manager Assistant with proxy line support. For more information on Cisco Unified Communications Manager Assistant with proxy line support, see the “Introducing Cisco Unified Communications Manager Assistant” section on page 11-5 and the “Related Topics” section on page 11-44.

Table 11-1 Cisco Unified Communications Manager Assistant Configuration Checklist with Proxy Line Support

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 If you have not already done so, configure the phones and users and</td>
<td>End User Configuration Settings, Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>and associate the devices to the users.</td>
<td>Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Associating Devices to an End User, Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>Administration Guide</td>
</tr>
<tr>
<td>Step 2 In Cisco Unified Serviceability, activate the Cisco IP Manager Assistant</td>
<td>Cisco Unified Serviceability Administration</td>
</tr>
<tr>
<td>service in the Service Activation window.</td>
<td>Guide</td>
</tr>
</tbody>
</table>

- Related Topics, page 11-44
Table 11-1  Cisco Unified Communications Manager Assistant Configuration Checklist with Proxy Line Support (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Configure system administration parameters:</td>
<td>Calling Search Space and Partitions, page 11-22</td>
</tr>
<tr>
<td>• Add three partitions.</td>
<td>Partition Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Add two calling search spaces.</td>
<td>Calling Search Space Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Add the CTI route point for Cisco Unified Communications Manager Assistant. You can have only one route point per server.</td>
<td>Cisco Unified Communications Manager Assistant CTI Route Point, page 11-23</td>
</tr>
<tr>
<td>• Configure Cisco IP Manager Assistant service parameters.</td>
<td>CTI Route Point Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Tip</strong> To automatically configure these system administration parameters, use the Cisco Unified Communications Manager Assistant Configuration Wizard. For more information, see the “Cisco Unified Communications Manager Assistant Configuration Wizard” section on page 11-19.</td>
<td>Cisco Unified Communications Manager Assistant Configuration Wizard, page 11-19</td>
</tr>
<tr>
<td>• Add the partition of the manager line to the calling search space of the Message Waiting Indicator (MWI) on and off number (if MWI is required).</td>
<td>Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 11-24</td>
</tr>
<tr>
<td>• If using the Cisco Unified Communications Manager intercom feature, add the Intercom partition, Intercom calling search space, Intercom directory number, and the Intercom translation pattern.</td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Message Waiting Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant, page 11-38</td>
</tr>
<tr>
<td></td>
<td>Intercom, page 28-1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, page 11-27</td>
</tr>
<tr>
<td>If multiple Cisco Unified Communications Manager Assistant pools are required to support large numbers of assistants and managers, configure the following Cisco IP Manager Assistant clusterwide service parameters:</td>
<td></td>
</tr>
<tr>
<td>• Enable Multiple Active Mode</td>
<td></td>
</tr>
<tr>
<td>• Pool 2 and Pool 3 Cisco IPMA Server IP Address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 11-24</td>
</tr>
<tr>
<td>Configure the application user CAPF profile (optional).</td>
<td>Security Considerations, page 11-28</td>
</tr>
<tr>
<td>Configure Cisco IP Manager Assistant service parameters for security (optional).</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Starting the Cisco IP Manager Assistant Service, page 11-29</td>
</tr>
<tr>
<td>Using the Serviceability Control Center Feature Services, stop and start the Cisco IP Manager Assistant service.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 11-1 Cisco Unified Communications Manager Assistant Configuration Checklist with Proxy Line Support (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>Configure phone parameters:</td>
<td></td>
</tr>
<tr>
<td>• Add Assistant Primary service as a Cisco Unified IP Phone service. If necessary, add Assistant Secondary service pointing to the Cisco Unified Communications Manager Assistant backup server as a Cisco Unified IP Phone service.</td>
<td>Cisco Unified IP Phone Service Configuration, page 11-29</td>
</tr>
<tr>
<td>• Check the Enable check box to activate the service.</td>
<td>IP Phone Service Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Configure Cisco Unified IP Phone.</td>
<td>Phone Button Template Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>Configure manager and assistant Cisco Unified IP Phone parameters:</td>
<td>Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Set up manager phone.</td>
<td></td>
</tr>
<tr>
<td>• Set up assistant phone.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>Configure manager phone settings:</td>
<td></td>
</tr>
<tr>
<td>• Assign a softkey template.</td>
<td>Manager and Assistant Phone Configuration, page 11-29</td>
</tr>
<tr>
<td>• If using Do Not Disturb, configure the Do Not Disturb fields on the manager phone.</td>
<td>Phone Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Add a primary line.</td>
<td>Configuring Cisco Unified IP Phones, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Set up voice-mail profile on primary line.</td>
<td>Directory Number Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Add intercom line.</td>
<td>Do Not Disturb, page 21-1</td>
</tr>
<tr>
<td>• For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.</td>
<td>Intercom, page 11-16</td>
</tr>
<tr>
<td>• For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975 add the intercom capabilities.</td>
<td>Intercom, page 28-1</td>
</tr>
<tr>
<td>• Subscribe to Cisco Unified IP Phone Service, Cisco Unified Communications Manager Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Cisco Unified Communications Manager Assistant Secondary Phone Service.</td>
<td>Configuring Speed-Dial Buttons or Abbreviated Dialing, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>• Set user locale.</td>
<td>Cisco Unified IP Phone Service Configuration, page 11-29</td>
</tr>
<tr>
<td>• Reset the phone.</td>
<td>Configuring IP Phone Services, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Tips About Resetting a Phone, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>To automatically configure some of the manager phone settings, choose the automatic configuration check box on the Manager Configuration window. For more information, see the “Manager Phones” section on page 11-30.</td>
<td></td>
</tr>
</tbody>
</table>
Introducing Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. When you configure Cisco Unified Communications Manager Assistant in proxy-line mode, the manager and assistant do not share a directory number. The assistant handles calls for a manager using a proxy number. The proxy number
is not the directory number for the manager, but an alternate number chosen by the system that an
assistant uses to handle manager calls. In proxy-line mode, a manager and an assistant have access to all
features that are available in Cisco Unified Communications Manager Assistant, which include default
assistant selection, assistant watch, call filtering, and divert all calls.

Table 11-1 lists the steps for configuring Cisco Unified Communications Manager Assistant with proxy
line support.

The following sections provide information about the Cisco Unified Communications Manager Assistant
feature:

- Cisco Unified Communications Manager Assistant Architecture Overview, page 11-6
- Cisco Unified Communications Manager Assistant Database Access Architecture, page 11-10
- Manager Interfaces, page 11-10
- Assistant Interfaces, page 11-10
- Softkeys, page 11-11
- Cisco Unified Communications Manager Assistant Administration Interface, page 11-11

Cisco Unified Communications Manager Assistant Architecture Overview

The Cisco Unified Communications Manager Assistant feature architecture comprises the Cisco IP
Manager Assistant service, the assistant console interfaces, and the Cisco Unified IP Phone interfaces.
See Figure 11-1.

Cisco IP Manager Assistant service routes calls that are presented to a CTI route point that is defined in
the Cisco IP Manager Assistant service parameters. See the “Setting the Service Parameters for Cisco
Unified Communications Manager Assistant” section on page 11-24.

Additional Information

See the “Related Topics” section on page 11-44.
Cisco Unified Communications Manager Assistant With Proxy Line Support

Introducing Cisco Unified Communications Manager Assistant

Cisco Tomcat loads the Cisco IP Manager Assistant service, a servlet. Cisco Tomcat gets installed at the Cisco Unified Communications Manager installation. The Cisco IP Manager Assistant service gets installed on all Cisco Unified Communications Manager servers in a cluster. After installation, the administrator activates the service from Serviceability, which automatically starts Cisco Unified Communications Manager Assistant. The Cisco IP Manager Assistant service checks to see whether it is one of the Cisco Unified Communications Manager Assistant servers that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the Cisco IP Manager Assistant service attempts to become the active Cisco IP Manager Assistant service. Currently, a Cisco Unified Communications Manager cluster supports only one active Cisco IP Manager Assistant service.

The Cisco IP Manager Assistant service performs the following tasks:

- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Contains the routing logic that applies filters on an incoming call for a manager. See Figure 11-2.
- Communicates to a Cisco Unified Communications Manager cluster through the Cisco CTIManager for third-party call control. Cisco Unified Communications Manager Assistant requires only one CTI connection for all users in a cluster.
- Accesses data from the database.
- Supports the Assistant Console application.

Cisco Unified Communications Manager supports redundancy of the Cisco IP Manager Assistant service. To achieve redundancy, you must configure a second Cisco IP Manager Assistant service in the same cluster.
Cisco Unified Communications Manager Assistant implements redundancy by using an active/standby server model. At any time, only one Cisco Unified Communications Manager Assistant server remains active and servicing all assistant console applications and phones. The other server stays in a standby mode and will detect failures on the active server. When it detects a failure, the backup server takes over and becomes the active server. All connections that were active get restored on the new server, and service continues uninterrupted to the users.

If the active server fails, the Assistant Console application fails over automatically to the backup server. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See Figure 11-3.
The Cisco IP Manager Assistant service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks non-authorized users who are posing as assistants.

**Assistant Console Interface**

Cisco Unified Communications Manager Assistant supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used to configure send all calls target, immediate divert target, and filters)

Administrators use Cisco Unified Communications Manager Administration, End User Configuration, to configure Cisco Unified Communications Manager Assistant for managers and assistants. See “Cisco Unified Communications Manager Assistant Administration Interface” section on page 11-11.

Cisco Unified Communications Manager makes all Cisco Unified Communications Manager Assistant manager features available through the Cisco Unified IP Phone, except manager configuration, which is available by using a browser. Assistants use the Cisco Unified IP Phone and the assistant console application. See “Manager Interfaces” section on page 11-10 and “Assistant Interfaces” section on page 11-10.

For more information about how to use the Cisco Unified Communications Manager Assistant features, see the *Cisco Unified Communications Manager Assistant User Guide*. 
Introducing Cisco Unified Communications Manager Assistant

Cisco Unified IP Phone Interface

Managers and assistants use softkeys and the Cisco Unified IP Phone Services button to access the Cisco Unified Communications Manager Assistant features. For more information about how to use the Cisco Unified Communications Manager Assistant phone features, see the Cisco Unified Communications Manager Assistant User Guide.

See “Manager Interfaces” section on page 11-10 and “Assistant Interfaces” section on page 11-10.

Cisco Unified Communications Manager Assistant Database Access

Architecture

The database stores all Cisco Unified Communications Manager Assistant configuration information. When the manager or assistant logs in, the Cisco IP Manager Assistant service retrieves all data that is related to the manager or assistant from the database and stores it in memory.

Manager Interfaces

The manager phone makes all manager features available with the exception of Manager Configuration. Cisco Unified Communications Manager Assistant automatically logs in a manager when the Cisco IP Manager Assistant service starts.

The manager can change selected assistants by using the Cisco Unified IP Phone Services button.

The manager accesses the Cisco Unified Communications Manager Assistant features Assistant Watch, Intercept Call, and Transfer to Voice Mail from the Cisco Unified IP Phone softkeys.

Note

Managers also have access to Cisco Unified Communications Manager features such as Do Not Disturb and iDivert.

The state of the features Assistant Watch, Do Not Disturb, Divert All Calls, and Filtering displays in the Status Window on the Cisco Unified IP Phone.

You can enable filtering and choose filter mode by using the Cisco Unified IP Phone Services button. Configuration of the filters occurs by using Manager Configuration. You can access the Manager Configuration on the assistant console by using a web browser (see the “Manager Configuration” section on page 11-43).

See the Cisco Unified Communications Manager Assistant User Guide for more information.

Assistant Interfaces

The assistant accesses the Cisco Unified Communications Manager Assistant features by using the Assistant Console application and the Cisco Unified IP Phone. The Assistant Console, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.
The Assistant Console displays the assistant lines and the manager proxy lines. A proxy line specifies a phone line that appears on the assistant Cisco Unified IP Phone. Assistants use the proxy lines to manage calls that are intended for a manager. For more information on setting up proxy lines, see the “Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant” section on page 11-38.

When the assistant logs in from the Assistant Console, the softkeys Redirect and Transfer to Voice Mail become active for the proxy lines. See the *Cisco Unified Communications Manager Assistant User Guide* for more information.

**Softkeys**

The Cisco Unified Communications Manager Assistant feature supports softkeys such as Redirect, Transfer to Voice Mail, and Do Not Disturb on the Cisco Unified IP Phone. Softkeys appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco Unified Communications Manager Assistant supports the following softkey templates:

- Standard Manager—Supports manager for proxy mode
- Standard Shared Mode Manager—Supports manager for shared mode
- Standard Assistant—Supports assistant in proxy or shared mode

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

*Note*

The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco Unified Communications Manager. Use Softkey Template configuration in Cisco Unified Communications Manager Administration to associate softkey templates with Cisco Unified Communications Manager Assistant devices and to create custom softkey templates. See **Softkey Template Configuration** in the *Cisco Unified Communications Manager Administration Guide*.

**Cisco Unified Communications Manager Assistant Administration Interface**

The administrator uses the End User Configuration window in Cisco Unified Communications Manager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant, configures an intercom line for the manager and assistant, and assigns a proxy line for a manager on the assistant phone.

See the “Manager and Assistant Configuration” section on page 11-33.
System Requirements for Cisco Unified Communications Manager Assistant with Proxy Line Support

Cisco Unified Communications Manager Assistant with proxy line support requires the following software components to operate:

- Cisco Unified Communications Manager
- Supported Browsers and platform:
  - Cisco Unified Communications Manager Assistant administration (using Cisco Unified Communications Manager Administration) and the Assistant Console are supported on Microsoft Internet Explorer (IE) 5.5 or later, Firefox 3.x or later, and Safari 4.x or later. (See the “Interactions and Restrictions” section on page 11-13 for more information.)
  - On a computer running Microsoft Windows 2000 or later, a customer can open one of the browsers specified above.
- Cisco Unified Communications Manager Bulk Administration Tool (BAT) if bulk adding of managers and assistants is planned.

Because Cisco Unified Communications Manager Assistant installs automatically on the same server with Cisco Unified Communications Manager, an additional server is not required.

To determine which Cisco Unified IP Phones support Cisco Unified Communications Manager Assistant, see the “Devices That Support Cisco Unified Communications Manager Assistant” section on page 11-12.

Devices That Support Cisco Unified Communications Manager Assistant

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support Cisco Unified Communications Manager Assistant. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
     - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
     - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
     - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click System Reports in the navigation bar.

3. In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.

4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

5. To generate a report of all IP Phones that support Cisco Unified Communications Manager Assistant, choose these settings from the respective drop-down list boxes and click the Submit button:
   - Product: All
Feature: IPMA

The List Features pane displays a list of all devices that support the Cisco Unified Communications Manager Assistant feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco Unified Communications Manager Assistant with proxy line support.

- Interactions, page 11-13
- Restrictions, page 11-16

Interactions

The following sections describe how Cisco Unified Communications Manager Assistant with proxy line support interacts with Cisco Unified Communications Manager applications and call processing:

- Bulk Administration Tool, page 11-13
- Calling Party Normalization, page 11-14
- Extension Mobility, page 11-14
- Internet Protocol Version 6 (IPv6), page 11-14
- Reporting Tools, page 11-14
- Multilevel Precedence and Preemption (MLPP), page 11-15
- Time-of-Day Routing, page 11-16
- Message Waiting Indicator, page 11-16
- Intercom, page 11-16

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

The BAT templates that are created by the Cisco Unified Communications Manager Assistant Configuration Wizard for Cisco Unified IP Phones support only the Cisco Unified Communications Manager intercom lines.

Additional Information

See the “Related Topics” section on page 11-44.
Chapter 11      Cisco Unified Communications Manager Assistant With Proxy Line Support

Interactions and Restrictions

Calling Party Normalization
Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Cisco Unified Communications Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs. For information on configuring calling party normalization, see the “Calling Party Normalization” section on page 8-1.

Extension Mobility
A manager who uses the Cisco Extension Mobility feature can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs into the Cisco Unified IP Phone by using extension mobility, and Cisco Unified Communications Manager Assistant service then automatically gets enabled on that phone. The manager can then access the Cisco Unified Communications Manager Assistant features.

To have access to Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, the administrator checks the Mobile Manager check box in the Manager Configuration window in Cisco Unified Communications Manager Administration (which is accessed from the End User Configuration window). See the “Configuring a Manager and Assigning an Assistant for Proxy Line Mode” section on page 11-34. For more information about configuring device profiles, see “Device Profile Configuration Settings” in the Cisco Unified Communications Manager Administration Guide. For more information about Cisco Unified Communications Manager Extension Mobility, see Chapter 9, “Cisco Extension Mobility.”

Internet Protocol Version 6 (IPv6)
Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

Reporting Tools
Cisco Unified Communications Manager Assistant provides statistical information in the CDR Analysis and Reporting (CAR) tool and provides a summary of changes to configurations in a change log. The following sections describe these reporting tools.

CDR Analysis and Reporting
Cisco Unified Communications Manager Assistant supports call-completion statistics for managers and assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR) tool supports call-completion statistics. Cisco Unified Serviceability supports inventory reporting. See the Cisco Unified Serviceability Administration Guide and the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide for more information.

IPMA_ChangeLog
The administrator can view a summary of changes that are made to the Manager or Assistant Configurations. A manager can change defaults by accessing the Manager Configuration from a URL. An assistant can change the manager defaults from the Assistant Console.
Interactions and Restrictions

Note

See the *Cisco Unified Communications Manager Assistant User Guide* for information about the URL and Manager Configuration.

When changes are made, the information gets sent to a log file that is called `ipma_changeLogxxx.log`. The log file resides on the server that runs the Cisco IP Manager Assistant service at the following location:

```
file get activelog tomcat/logs/ipma/log4j
```

The administrator can download this file from the server by using the Trace Collection Tool in the Cisco Unified Real Time Monitoring Tool. See the *Cisco Unified Real Time Monitoring Tool Administration Guide* for more information.

The log file contains the following fields:

- **LineNumber**—The line in the log file with information about changes
- **TimeStamp**—The time that the configuration changed
- **for Manager/Assistant**—Designation of whether the change is for the manager or the assistant
- **for Userid**—The userid of the manager or assistant that is being changed
- **by Manager/Assistant**—Designation of whether the manager or the assistant made the change
- **by Userid**—The userid of the manager or assistant who made the change
- **Parameter Name**—What changed; for example, divert target number
- **Old Value**—The value of the information before the change
- **New Value**—The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

**Procedure**

1. Start the Microsoft Excel application.
2. To open the ConfigChange*.log file, choose **File > Open**.
3. Choose the **Original data type**, file type as Delimited, and click **Next**.
4. Choose Delimiters as Comma and click **Next**.
5. When complete, click **Finish**.

**Multilevel Precedence and Preemption (MLPP)**

The following points describe the interactions between Cisco Unified Communications Manager Assistant with proxy line support and MLPP:

- Cisco Unified Communications Manager Assistant preserves call precedence in the handling of calls. For example, when an assistant diverts a call to a manager, Cisco Unified Communications Manager Assistant preserves the precedence of the call.
- Filtering of precedence calls occurs in the same manner as all other calls. The precedence of a call will not affect whether a call is filtered.
Because Cisco Unified Communications Manager Assistant does not perceive the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

**Time-of-Day Routing**

Time-of-Day routing routes calls to different locations based on the time that the call gets made; for example, during business hours, calls get routed to a manager office, and after hours, the calls go directly to voice-messaging service.

Partitions specify the time schedule and time zone that Time-of-Day routing uses. Cisco Unified Communications Manager Assistant partitions and partitions in Cisco Unified Communications Manager Assistant calling search spaces support Time-of-Day routing.

For more information about Time-of-Day routing, see Time-of-Day Routing in the Cisco Unified Communications Manager System Guide.

**Message Waiting Indicator**

The Message Waiting Indicator (MWI) on and off numbers should have the partition of the manager line in their calling search space. The partition can exist in any order of priority within each calling search space. For more information on configuring message waiting indicators, see “Message Waiting Configuration Settings” in the Cisco Unified Communications Manager Administration Guide.

**Intercom**

Cisco Unified Communications Manager Assistant supports the following intercom features:

- Cisco Unified Communications Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). This intercom feature gets configured by using the DN configuration and end user (manager and assistant) configuration windows.

- Cisco Unified Communications Manager intercom (used with Cisco Unified IP Phones 7900 except 7940 and 7960). This intercom feature gets configured by using the intercom partition, intercom calling search space, intercom directory number, intercom translation pattern, DN, and end user (manager and assistant) configuration windows.

**Restrictions**

The following restrictions apply to Cisco Unified Communications Manager Assistant:

- Cisco Unified Communications Manager Assistant supports SIP on Cisco Unified IP Phones 7900 series except the Cisco Unified IP Phone 7940 and 7960.

- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants by configuring multiple Cisco IP Manager Assistant servers (pools). When multiple pools are enabled, a manager and all configured assistants for that manager should belong to the same pool.

- One manager can have up to 10 assigned assistants.

- One assistant can support up to 33 managers (if each manager has one Cisco Unified Communications Manager Assistant—Controlled Line).
Installing and Activating Cisco Unified Communications Manager Assistant

Cisco Tomcat loads the Cisco Unified Communications Manager Assistant, a servlet. Cisco Tomcat gets installed and started at Cisco Unified Communications Manager installation. For more information, see the “Cisco Unified Communications Manager Assistant Architecture Overview” section on page 11-6.

The administrator performs three steps after installation to make Cisco Unified Communications Manager Assistant available for system use:

1. Use Cisco Unified Serviceability Service Activation, located on the Tools menu, to activate the Cisco IP Manager Assistant service. See the Cisco Unified Serviceability Administration Guide.

2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24.

3. Use the Serviceability Control Center Feature Service window to stop and start the Cisco IP Manager Assistant service. See the “Starting the Cisco IP Manager Assistant Service” section on page 11-29.

Note: If the managers and assistants will require Cisco Unified Communications Manager Assistant features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco Unified Communications Manager Assistant. See the Cisco Unified Communications Operating System Administration Guide for information on locale installers.
Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

For successful configuration of Cisco Unified Communications Manager Assistant, review the steps in the configuration checklist, perform the system, user, and device configuration requirements, and configure the managers and assistants.

Note
Cisco Unified Communications Manager Assistant with proxy line support coexists in the same Cisco Unified Communications Manager cluster with Cisco Unified Communications Manager Assistant with shared line support. For configuration information about shared line support, see Configuring Cisco Unified Communications Manager Assistant with Shared Line Support.

The following sections provide configuration information:
- System Configuration with Proxy Line Support, page 11-18
- Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 11-24
- Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, page 11-27
- Security Considerations, page 11-28
- Starting the Cisco IP Manager Assistant Service, page 11-29
- Cisco Unified IP Phone Service Configuration, page 11-29
- Manager and Assistant Phone Configuration, page 11-29
- Manager and Assistant Configuration, page 11-33

Tip
Before you configure the Cisco Unified Communications Manager Assistant with proxy line support, review the “Configuration Checklist for Cisco Unified Communications Manager Assistant with Proxy Line Support” section on page 11-2.

System Configuration with Proxy Line Support

Because the Cisco IP Manager Assistant service intercepts calls that are made to managers who are using proxy line mode, it requires configuration of partitions, calling search spaces, and route points. For more information on configuring Cisco Unified Communications Manager Assistant, see the “System Configuration with Proxy Line Support” section on page 11-18.

You must perform the following configurations before you configure devices and users for Cisco Unified Communications Manager Assistant:
- Calling Search Space and Partitions, page 11-22
- Cisco Unified Communications Manager Assistant CTI Route Point, page 11-23

Cisco Unified Communications Manager Assistant provides a one-time-use configuration wizard that helps the administrator configure partitions, calling search spaces, a route point, and the Cisco Unified Communications Manager Assistant phone service. The Cisco Unified Communications Manager Assistant Configuration Wizard also creates the Cisco IP Manager Assistant service parameters in the
Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the “Cisco Unified Communications Manager Assistant Configuration Wizard” section on page 11-19.

Note
This document provides specific information about Cisco Unified Communications Manager Assistant configuration. For more information about configuring Calling Search Spaces, Partitions, and CTI Route Points, see the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager Assistant Configuration Wizard

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. Table 11-1 lists the steps for configuring Cisco Unified Communications Manager Assistant with proxy line support. Table 12-1 lists the steps for configuring Cisco Unified Communications Manager Assistant with proxy line support.

With the Cisco Unified Communications Manager Assistant Configuration Wizard, configuration takes less time and eliminates errors. The partitions, calling search spaces, and route point automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the manager phone, the assistant phone, and all other user phones. The administrator can use the BAT templates to configure the managers, assistants, and all other users. See the Cisco Unified Communications Manager Bulk Administration Guide.

Note
The Cisco Unified Communications Manager Assistant Configuration Wizard only creates the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section of the Service Parameters Configuration window. You must enter the remaining service parameters manually. For service parameter information, see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24.

The Cisco Unified Communications Manager Assistant Configuration Wizard provides windows for each configuration parameter. The windows provide the administrator with preconfigured information. If the administrator prefers to use other configuration information (for example, partition names), the administrator can change the preconfigured information to the appropriate information.

Perform the following procedure to configure the Cisco Unified Communications Manager Assistant system parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard.

Before You Begin
Ensure that the configuration wizard runs from the same server (the Cisco Unified Communications Manager server) as the Bulk Administration Tool (BAT).

You can run the wizard only one time.

Procedure

Step 1
From Cisco Unified Communications Manager Administration, choose Application > Cisco Unified CM Assistant Configuration Wizard.

The Cisco Unified Communications Manager Assistant Configuration Wizard Overview window displays and provides a description of the configuration wizard process.
You can use the Cisco Unified Communications Manager Assistant Configuration Wizard only once in a Cisco Unified Communications Manager cluster configuration. The feature verifies the number of times that the configuration wizard has been run (zero or 1). If the configuration wizard has been run once, the summary window automatically displays. The summary window displays the details and status of the configuration wizard that was previously run. If the configuration has not been run, the configuration process continues.

Step 2
To begin the Cisco Unified Communications Manager Assistant Configuration wizard process, click the Next button.

The Partition for Managers window displays.

Step 3
Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 4
Click the Next button.

The CTI Route Point Partition window displays.

Step 5
Enter a name in the CTI route point name field and provide a description; otherwise, use the default CTI route point name.

Step 6
Click the Next button.

The Partition for All Users window displays.

Step 7
Enter a name in the partition name field and provide a description; otherwise, use the default partition name and description.

Step 8
Click the Next button.

The Intercom Partition window displays.

Step 9
Enter a name in the name field and provide a description; otherwise, use the default Intercom Partition name.

Step 10
Click the Next button.

The Assistant Calling Search Space window displays.

Step 11
Enter a name in the name field and provide a description; otherwise, use the default calling search space name and description.

The Available Partitions and Selected Partitions boxes under the Route Partitions for this Calling Search Space automatically list Partitions for the Assistant Calling Search Space. If the defaults that are provided are not wanted, the administrator can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 12
Click the Next button.

The Everyone Calling Search Space window displays.

Step 13
Enter a name in the name field and provide a description; otherwise, use the default calling search space name and description.

The Available Partitions and Selected Partitions boxes under the Additional Route Partitions for This Calling Search Space automatically list Partitions for the Everyone Calling Search Space. If the defaults that are provided are not wanted, the administrator can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 14
Click the Next button.
Cisco Unified Communications Manager Assistant With Proxy Line Support

Chapter 11  Cisco Unified Communications Manager Assistant With Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

If you have existing calling search spaces that are configured in the system, the Existing Calling Search Spaces window displays; otherwise, the Existing Calling Search Spaces window does not display (proceed to Step 15).

Cisco Unified Communications Manager Assistant requires that existing calling search spaces add the prefix Generated_Route Point and Generated_Everyone partitions. The Available Calling Search Spaces and Selected Calling Search Spaces boxes automatically list these partitions. Use the up and down arrows to move partitions from one box to the other.

Note

The prefix that is added to the existing calling search spaces may change if the administrator has changed the names of the partitions in Steps 10 and 12.

Step 15  Click the Next button.

The CTI Route Point window displays.

Step 16  Enter a name in the CTI route point name field; otherwise, use the default CTI route point name.

Step 17  From the drop-down selection list box, choose the appropriate device pool.

Step 18  Enter a route point directory number; otherwise, use the default route point directory number.

Step 19  From the drop-down selection list box, choose the appropriate numbering plan.

Step 20  Click the Next button.

The Phone Services window displays.

Step 21  Enter the Primary Phone Service Name; otherwise, use the default Phone Service name.

Step 22  From the drop-down list box, choose the Primary Cisco Unified Communications Manager Assistant server or enter a server name or IP address.

Step 23  Enter the Secondary Phone Service Name; otherwise, use the default Phone Service name.

Step 24  From the drop-down list box, choose the secondary Cisco Unified Communications Manager Assistant server or enter a server name or IP address.

Step 25  Click the Next button.

The Confirmation window displays. It provides all the information that the administrator chose while using the configuration wizard. If the information is not correct, the administrator can cancel the configuration process or return to the previous configuration windows by pressing the Back button.

Step 26  To allow the configuration process to execute, click the Finish button; otherwise, to cancel the configuration process, click the Cancel button.

Upon completion, a final status window displays. The window shows the success or failure of each part of the wizard.

Any errors that the configuration wizard generates get sent to a trace file. Access this file by using the following CLI command:

```
file get activelog tomcat/logs/ccmadmin/log4j
```

With the data that is collected from the configuration windows, the wizard automatically creates the partitions, calling search spaces, a route point, and the Cisco Unified Communications Manager Assistant phone services. The wizard populates the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section of the Service Parameters Configuration window. Additionally, the wizard creates the manager phone template, the assistant phone template, and the Everyone phone template that BAT uses to configure phones for
use with Cisco Unified Communications Manager Assistant. See the *Cisco Unified Communications Manager Bulk Administration Guide* for information about configuring the manager and assistant devices.

---

### Calling Search Space and Partitions

A Cisco Unified Communications Manager Assistant route point (called CTI route point) intercepts calls for the managers and determines where to route them; therefore, all calls for the managers should flow through the route point first.

To accomplish the call flow, Cisco Unified Communications Manager Assistant uses calling search spaces. Calls from lines that the Cisco IP Manager Assistant service must route or act upon should have a calling search space that has the route point partition (you can call this partition CTI Route Point) that is configured as the primary partition, and you can call the secondary partition the Everyone partition. See the following example.

**Note**

For a manager who has multiple lines and who uses proxy line support, those lines must fall in the range that is covered by the route point (for example, a route point of 1xxx means that manager lines must fall in 1000 - 1999 range).

**Example**

A user (in Everyone partition) places a call to a manager primary line (in Manager partition). Because the partition for the originating call does not include the manager primary line, the manager line number gets searched through the calling search space. The order of priority of the partitions in the calling search space provides basis for the search. Because the user line has a calling search space that comprises CTI Route Point and Everyone, the search for the manager primary line begins with the CTI route point partition. Because the CTI route point matches the manager primary number, the call gets presented to the route point. The Cisco IP Manager Assistant service that is monitoring the route point gets the call and routes the call by using the manager settings.

All lines that have calls that should go through a route point should have a calling search space that is called Cisco Unified Communications Manager Assistant and Everyone. Examples of lines that require this calling search space configuration include manager primary and private lines, assistant primary line, and all other user lines.

All lines that have calls that should go directly to the manager without having the routing logic applied on them should have a calling search space that is called Managers and Everyone. Examples of lines that require this calling search space configuration include Cisco CTI route point and assistant proxy lines.
See Figure 11-4 for an example of the calling search space and partition configuration.

**Figure 11-4** Cisco Unified Communications Manager Assistant Calling Search Space and Partition Configuration Example for Proxy Line Support

**Configuration Tips**
- Create three partitions that are called CTI Route Point, Manager, and Everyone.
- Create a calling search space that is called CSS-M-E, which contains the partitions Manager and Everyone.
- Create a calling search space that is called CSS-I-E, which contains the partitions CTI Route Point and Everyone.
- Configure the manager primary and private directory numbers (DN) in the partition that is called Manager.
- Configure all assistants lines and other users lines in the partition that is called Everyone.
- Configure the Cisco Unified Communications Manager Assistant route point in the partition that is called CTI Route Point.
- Configure the MWI On/Off numbers with a calling search space CSS-M-E.

**Cisco Unified Communications Manager Assistant CTI Route Point**

You can have only one Cisco Unified Communications Manager Assistant CTI route point for each server. The directory numbers of CTI route points must match the primary and private directory numbers of the manager; otherwise, the Cisco IP Manager Assistant service routes calls inappropriately. Cisco recommends the use of wild cards to satisfy this condition.

When you add directory number ranges for the CTI route point, the caller search space must not contain the Manager partition because Cisco Unified Communications Manager always matches on the most specific match regardless of partition order; for example, the manager line is 1000, and the directory number range that is added to the route point is 1xxx. If a caller search space includes the Manager
partition, even when the CTI Route Point partition is at the top, the more specific match applies for the manager directory number, and the call does not get routed by Cisco Unified Communications Manager Assistant but gets sent directly to the manager extension. For Cisco Unified Communications Manager Assistant to route the call when using directory number ranges on the route point, the caller search space must include the CTI Route Point partition but not the Manager partition.

Configuration Tips

- Create a CTI route point that is called Assistant_RP.
- Configure the directory numbers of the route point to match the primary and private directory numbers of the managers (for example, for managers whose primary directory numbers are 1000-1999, create a route point DN as 1xxx for line 1; for managers whose primary directory numbers are 2000-2999, create a route point DN as 2xxx for line 2). Configure the directory numbers in the CTI Route Point partition with a calling search space of CSS-M-E.
- Configure Call Forward No Answer with Destination Internal/External as Route Point DN (for example, CFNA as 1xxx for the Route Point DN 1xxx) with a calling search space of CSS-M-E. Call Forward No Answer forwards the call to the manager if the Cisco IP Manager Assistant service is not available.

Setting the Service Parameters for Cisco Unified Communications Manager Assistant

Service parameters for the Cisco IP Manager Assistant service comprise two categories: general and clusterwide. Specify clusterwide parameters once for all Cisco IP Manager Assistant services. Specify general parameters for each Cisco IP Manager Assistant service that is installed.

Set the Cisco IP Manager Assistant service parameters by using Cisco Unified Communications Manager Administration to access the service parameters (System > Service Parameters). Choose the server where the Cisco Unified Communications Manager Assistant application resides and then choose the Cisco IP Manager Assistant service.

Cisco IP Manager Assistant includes the following service parameters that must be configured:

- Clusterwide
  - Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address. To avoid potential high CPU usage, enter the address of the local CTIManager server where the IPMA process is running when you configure the Cisco IP Manager Assistant CTIManager (Primary) IP Address service parameter.
  - Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server Port—Default specifies Port 2912.
  - Cisco IPMA Assistant Console Heartbeat Interval—Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
  - Cisco IPMA Assistant Console Request Timeout—Default specifies 30 seconds.
  - Cisco IPMA RNA Forward Calls—Default specifies False. If the parameter is set to True, an assistant phone that does not get answered will forward to another assistant phone.
Cisco IPMA RNA Timeout—Default specifies 10 seconds. RNA timeout specifies how long an assistant phone can go unanswered before the call is forwarded to another assistant phone. If Call Forward No Answer (CFNA) and RNA timeout are both configured, the first timeout occurrence takes precedence.

CTIManager Connection Security Flag has the following two options:

- Nonsecure—The security mode specifies nonsecure.
- Use Cluster Default—Cisco IP Manager Assistant service fetches the security mode for the cluster. If the cluster security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.

Note: Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.

Advanced Clusterwide

- Enable Multiple Active Mode—The default specifies False. When set to True, the administrator can configure up to 7000 managers and assistants by using multiple pools.

Cisco IPMA Service Parameters for each server

- CTIManager (Primary) IP Address—No default. Enter the IP address of the primary CTIManager that will be used for call control.
- CTIManager (Backup) IP Address—No default. Administrator must manually enter this IP address.
- Route Point Device Name for Proxy Mode—No default. Choose the Cisco Unified Communications Manager Assistant route point device name (that you configure by using Device > CTI Route Point).
- CAPF Profile Instance Id for Secure Connection to CTIManager—This service parameter specifies the Instance Id of the Application CAPF Profile for the Application User IPMASecureSysUser that this Cisco Unified Communications Manager Assistant server will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.
Cisco Unified Communications Manager Assistant includes the following clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants:

- **Softkey Templates**
  - Assistant Softkey Template—Default specifies Standard Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during assistant automatic configuration.
  - Manager Softkey Template for Proxy Mode—Default specifies Standard Manager softkey template. This parameter specifies the softkey template that is assigned to the manager device during manager automatic configuration.
  - Manager Softkey Template for Shared Mode—Default specifies Standard Shared Mode Manager. This service parameter does not apply to proxy line support.

- **IPMA Device Configuration Defaults**
  - Manager Partition—No default. This parameter specifies the partition that the automatic configuration assigns to the manager line(s) that Cisco Unified Communications Manager Assistant handles on the manager device. Enter a partition that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
  - All User Partition—No default. This parameter specifies the partition that the automatic configuration assigns to the proxy line(s) and the intercom line on the assistant device as well as the intercom line on the manager device. Enter a partition that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
  - IPMA Calling Search Space—No default. This parameter specifies the calling search space that the automatic configuration assigns to the manager line(s) that Cisco Unified Communications Manager Assistant handles and the intercom line on the manager device as well as the assistant intercom line on the assistant device. Enter a calling search space that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
  - Manager Calling Search Space—No default. This parameter specifies the calling search space that the automatic configuration assigns to the proxy line(s) on the assistant device. Enter a calling search space that exists in the system. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
  - Cisco IPMA Phone Service—No default. This parameter specifies the IPMA phone service that the automatic configuration assigns to the manager device. If you run the Cisco Unified Communications Manager Assistant Configuration Wizard, the wizard populates this value.
  - IPMA Secondary Phone Service—No default. This parameter specifies a secondary IPMA phone service that the automatic configuration assigns to the manager device if the primary service is not available.

**Note**
If you change the IPMASEcureSysUser password, you must then go to the IPMASEcureSysUser config > CAPF Profile config window for the profile that was selected on the IPMA Service Parameters window, change the Certificate Operation to “Install/Upgrade”, provide the authentication string, and restart the IPMA service.
• Proxy Directory Number Range
  - Starting Directory Number—No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the assistant configuration. The Starting Directory Number parameter specifies the first directory number in the range. The next available number in the range displays in the Proxy Line field in the End User Configuration window when you are configuring an assistant.
  - Ending Directory Number—No default. The Starting Directory Number and the Ending Directory Number parameters provide a range of proxy numbers that are available for the assistant configuration. The Ending Directory Number parameter specifies the last directory number in the range. If you enter a smaller value in the Ending Directory Number field than you do in the Starting Directory Number field, a message displays when you access the Assistant Configuration in the End User Configuration window.

• Proxy Directory Number Prefix
  - Number of Characters to be Stripped from Manager Directory Number—Default specifies 0. This parameter specifies the number of characters that Cisco Unified Communications Manager strips from a manager directory number (DN) in the process of generating a proxy DN. You can use this parameter along with the Prefix for Manager Directory Number parameter to generate a proxy DN. For example, if you strip 2 digits from a manager DN of 2002 and add a prefix of 30 (specified in the Prefix for Manager Directory Number service parameter), Cisco Unified Communications Manager generates a proxy DN of 3002. You can strip 0 to 24 characters.
  - Prefix for Manager DN—No default. This parameter specifies the prefix that Cisco Unified Communications Manager adds to a manager DN in the process of generating the proxy DN. For example, if manager DN is 1001, number of characters to be stripped is 0, and the prefix is *, Cisco Unified Communications Manager generates a proxy DN of *1001. The maximum prefix length equals 24.

Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability

Cisco Unified Communications Manager supports up to 3500 managers and 3500 assistants for a total of 7000 users. To support 7000 users, the administrator must configure multiple active Cisco IP Manager Assistant servers by enabling and setting service parameters. Administrators can configure up to three active Cisco IP Manager Assistant servers, each managing up to 2500 managers and assistants. Each server can also have a backup server. Configure the Cisco IP Manager Assistant servers by using the Advanced Service Parameters, Enable Multiple Active Mode, Pool 2: Cisco IPMA Server, and Pool3: Cisco IPMA Server. See the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24 for more information. See Figure 11-5.
1. Activate IPMA service (see the “Installing and Activating Cisco Unified Communications Manager Assistant” section on page 11-17)

2. Enable multiple active mode (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24)

3. Provide IP addresses for multiple pools (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24)

4. Add the pool to the manager/assistant from the End User Configuration window (see the “Configuring a Manager and Assigning an Assistant for Proxy Line Mode” section on page 11-34)

Migration Considerations
If you are migrating from a release previous to Cisco Unified Communications Manager Release 8.0(2), all managers and assistants will get migrated to Pool 1 (the default).

Security Considerations
Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection).
Chapter 11  Cisco Unified Communications Manager Assistant With Proxy Line Support

Managing Cisco Unified Communications Manager Assistant With Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

The administrator must configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node) by choosing User Management > Application User CAPF Profile. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses IPMASecureSysUser.

For more information about configuring security for Cisco Unified Communications Manager Assistant, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24.

The Cisco Unified Communications Manager Security Guide provides detailed security configuration procedures for CTI applications.

Starting the Cisco IP Manager Assistant Service

The Cisco IP Manager Assistant service runs as an application on Cisco Tomcat. To start or stop the Cisco IP Manager Assistant service, use the Serviceability Control Center Feature Services window.

Cisco Unified IP Phone Service Configuration

Add the Cisco IP Manager Assistant service as a new Cisco Unified IP Phone Service. Configure a name, description, and the URL for the Cisco IP Manager Assistant service. The name and description that you enter should be in the local language because it displays on the manager Cisco Unified IP Phone. For more information, see IP Phone Services Configuration in the Cisco Unified Communications Manager Administration Guide.

Provide a URL by using the format http://<server-ipaddress>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME# For example http://123.45.67.89:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

Configuration Tips

To provide redundancy for the Cisco Unified IP Phone Service, create a Cisco Unified IP Phone Service that uses the host name rather than the IP address. The host name in DNS should resolve to both Cisco Unified Communications Manager Assistant primary and backup IP addresses. The phone functionality for softkeys and filtering, as well as the phone service, will fail over automatically in the case of a failover.

Manager and Assistant Phone Configuration

You must configure devices for each manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco Unified IP Phone 7940, 7942, 7945, 7960, 7962, 7965, and 7975 (SCCP and SIP)

- Add a Cisco Unified IP Phone 7900 series for each manager and assistant that will be using Cisco Unified Communications Manager Assistant. To add these phones, use one of the following methods:
  - Manually (Device > Phone)
Chapter 11      Cisco Unified Communications Manager Assistant With Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Auto registration
BAT
• Assign the Standard Assistant or Standard Manager softkey template.

Cisco Unified IP Phone 7940
You can use the Cisco Unified IP Phone 7940, 7942, or 7945 for Cisco Unified Communications Manager Assistant, but certain restrictions apply.
• Add a Cisco Unified IP Phone 7940, 7942, or 7945 for each manager with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for manager with shared line support
• Add a Cisco Unified IP Phone 7940 for each assistant with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for assistant

Note Cisco recommends the Cisco Unified IP Phones 7960, 7962, 7965, and 7975 because they provide more functionality.

Note Cisco Unified IP Phones 7940 and 7960 support only the Cisco Unified Communications Manager Assistant intercom feature.

After you complete these tasks, configure the phones as described in the following sections:
• Manager Phones, page 11-30
• Assistant Phones, page 11-31
• Nonmanager and Nonassistant Phones, page 11-33

Manager Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and tips for configuring a manager phone.

Manager Phone Configuration
Configure the manager Cisco Unified IP Phones with the following settings:
• Standard Manager softkey template
• Primary line
• Additional lines if required
• Voice-messaging profile on primary line
• If using the Cisco Unified IP Phone 7900 series, except Cisco Unified IP Phone 7940 or 7960, configure the intercom feature
• If using the Cisco Unified IP Phone 7940 or 7960, configure the incoming intercom line to support the auto answer with speakerphone or headset option
Chapter 11  Cisco Unified Communications Manager Assistant With Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

- If using the Cisco Unified IP Phone 7940 or 7960, configure the speed dial for outgoing intercom targets.
- Subscribe to Cisco Unified IP Phone Service, Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Assistant Secondary Phone Service.
- Set user locale

You can automate some of these settings by choosing the Automatic Configuration check box on the Manager Configuration window when you configure the manager. Automatic Configuration sets the following items for the manager device or device profile:

- Softkey template
- Subscription to Cisco Unified Communications Manager Assistant phone service
- Calling search space and partition for Cisco Unified Communications Manager Assistant-controlled selected lines and intercom line (applies only to Cisco Unified IP Phone 7940 and 7960)
- Auto answer with speakerphone for intercom line (applies only to Cisco Unified IP Phone 7940 and 7960)

Before you can automatically configure a manager phone, you must set the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. These parameters specify information such as which partition and calling search space to use for a manager line. You can enter these parameters manually, or you can populate the parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard. For more information about these parameters, see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the “Cisco Unified Communications Manager Assistant Configuration Wizard” section on page 11-19.

After you enter the appropriate service parameters, you can automatically configure a manager phone by choosing the Automatic Configuration check box on the Manager Configuration window and clicking Save. For step-by-step instructions, see the “Configuring a Manager and Assigning an Assistant for Proxy Line Mode” section on page 11-34.

Configuration Tips for Manager

- Do not configure Call Forward All Calls on the manager primary DN because the manager cannot intercept calls that are routed to the assistant proxy DN when Call Forward All Calls is set.
- Configure primary lines (Cisco Unified Communications Manager Assistant-controlled lines) and assign DNs; use the Managers partition and the CSS-I-E calling search space for these lines if you are not using the automatic configuration.
- If the manager is using the Cisco Unified IP Phone 7940 or 7960, configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if you are not using the automatic configuration.
- If the manager is using the Cisco Unified IP Phone 7900 series (except Cisco Unified IP Phone 7940 and 7960) and requires intercom, add the intercom DN and choose the applicable intercom partition and intercom calling search space.

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940, 7942, and 7945. For more information, see the “Cisco Unified IP Phone 7940” section on page 11-30.

Assistant Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and provides tips for configuring an assistant phone.
## Assistant Phone Configuration

Configure the assistant Cisco Unified IP Phones with the following settings:

- Standard Assistant softkey template
- Default expansion module (optional)
- Standard Assistant phone button template (if using an expansion module)
- Primary line
- Proxy lines for each configured manager with a voice-mail profile that is the same as the manager voice-mail profile
- Incoming intercom line to support the auto answer with speakerphone or headset option (applies only to Cisco Unified IP Phone 7940 and 7960)
- Speed dial to incoming intercom line for each configured manager (applies only to Cisco Unified IP Phone 7940 and 7960)
- Set user locale
- Subscribe to Cisco Unified IP Phone Service, Assistant Primary Phone Service. If necessary, subscribe to Cisco Unified IP Phone Service, Assistant Secondary Phone Service.

You can automate some settings by choosing the Automatic Configuration check box on the Assistant Configuration window when you configure the assistant. Automatic Configuration sets the following items for the assistant device or device profile:

- Softkey template
- Phone button template
- Calling search space and partition for existing proxy lines and intercom line
- Auto answer with speakerphone for intercom line
- Autogenerated proxy lines creation, if chosen

Before you can automatically configure an assistant phone, you must set the Cisco IP Manager Assistant service parameters in the Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode) section. These parameters specify information such as which partition and calling search space to use for assistant proxy and intercom lines. You can enter these parameters manually, or you can populate the parameters by using the Cisco Unified Communications Manager Assistant Configuration Wizard. For more information about these parameters, see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24. For more information on the Cisco Unified Communications Manager Assistant Configuration Wizard, see the “Cisco Unified Communications Manager Assistant Configuration Wizard” section on page 11-19.

After you have entered the appropriate service parameters, you can automatically configure an assistant phone by choosing the **Automatic Configuration** check box on the Assistant Configuration window. For step-by-step instructions, see the “Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant” section on page 11-38.

Automatic configuration allows you to create a proxy line automatically (with the required calling search space and partition information) on the assistant phone. The autogenerated proxy numbers get generated from the values that you enter for the Proxy Directory Number Range and Proxy Directory Number Prefix service parameters as described in the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24.

Autogenerated numbers appear along with lines on the assistant device in the Proxy Line drop-down list box on the Assistant Configuration window when you configure the assistant. “Line” appears before existing lines on the assistant phone. “Auto” appears before each autogenerated number until the system adds that proxy line to an assistant phone. The system sets the calling search space and partition for the
proxy line and the intercom line, if any, on the basis of the Cisco IP Manager Assistant service parameter settings. For step-by-step instructions, see the “Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant” section on page 11-38.

**Configuration Tips for Assistant**

- If the assistant is using the Cisco Unified IP Phone 7940 or 7960, configure an incoming intercom line and assign a DN; use the Everyone partition and the CSS-I-E calling search space if you are not using the automatic configuration.
- If the assistant is using the Cisco Unified IP Phone 7900 series (except 7940 and 7960) and requires intercom, add the intercom DN and choose the applicable intercom partition and intercom calling search space.
- Configure a proxy line and assign a DN for each manager that the assistant will support; use the Everyone partition and the CSS-M-E calling search space if you are not using the automatic configuration.

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940, 7942, and 7945. For more information, see the “Cisco Unified IP Phone 7940” section on page 11-30.

**Nonmanager and Nonassistant Phones**

In addition to configuring manager and assistant devices, configure all other users in the Cisco Unified Communications Manager cluster. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the cluster.

**Configuration Tips for Nonmanager and Nonassistant**

- Use the Everyone partition for all other users.
- Use the CSS-I-E calling search space for all other users.
- If you use auto registration, perform the following tasks:
  - On the Device Pool Configuration window (System > Device Pool), choose CSS-I-E from the Calling Search Space for Auto-registration field.
  - On the Cisco Unified CM Configuration window (System > Cisco Unified Communications Manager), choose Everyone from the Partition field.
- If you use BAT, you can use the Everyone template that the Cisco Unified Communications Manager Assistant Configuration Wizard created to add phones in the Everyone partition and the CSS-I-E calling search space.

**Manager and Assistant Configuration**

From the Cisco Unified Communications Manager End User Configuration window, configure the settings for the managers and assistants who use the Cisco Unified Communications Manager Assistant feature. You can configure Cisco Unified Communications Manager Assistant in proxy line or shared line mode. To configure the manager and assistant in proxy line mode, see the “Configuring a Manager and Assigning an Assistant for Proxy Line Mode” section on page 11-34. To configure the manager and assistant for shared line mode, see the “Configuring a Manager and Assigning an Assistant for Shared Line Mode” section on page 12-22.
From the End User Configuration window, perform the following functions:

- Choose manager and assistant devices.
- Automatically configure a manager or assistant device, if you want one.
- Choose the local language in which the End User Configuration window displays.
- Choose the Manager Configuration or Assistant Configuration window to configure the following Cisco Unified Communications Manager Assistant settings:
  - Set up primary and incoming intercom lines for intercom capability. For example, configure extension 3102 as the intercom line for the manager. This line will receive intercom calls from the assistant; for example, the assistant line 1 (1102) and line 2 (1103) display on the assistant console, and the assistant answers them.

Note

The intercom line that you choose will be the one that you created by using the Cisco Unified Communications Manager intercom feature (applicable only to Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975) or by using speed dials (applicable only to Cisco Unified IP Phones 7940 and 7960).

- Configure assistant information for managers.
- Set up proxy lines for each manager on the assistant phone. For example, assistant lines 4 and 5 take calls from manager lines 1102 and 1103.

The following sections provide details about configuring the manager and assistant settings:

- Configuring a Manager and Assigning an Assistant for Proxy Line Mode, page 11-34
- Deleting Cisco Unified Communications Manager Assistant Information from the Manager, page 11-36
- Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant, page 11-38
- Deleting the Cisco Unified Communications Manager Assistant Information from the Assistant, page 11-39
- Intercom, page 28-1

### Configuring a Manager and Assigning an Assistant for Proxy Line Mode

Perform the following procedure to configure a manager and assign an assistant to the manager. To configure a new user, see “End User Configuration Settings” in the Cisco Unified Communications Manager Administration Guide.

Tip

Configure manager information before configuring assistant information.

**Procedure**

**Step 1**

To configure the manager and to assign an assistant to an existing user, choose User Management > End User.

**Step 2**

To find the user that will be the Cisco Unified Communications Manager Assistant manager, click the Find button or enter the user name in the Search Options field and click the Find button.
Step 3  To display user information for the chosen manager, click the user name. The End User Configuration window displays.

Step 4  To configure Cisco Unified Communications Manager Assistant information for the manager, choose Manager Configuration from the Related Links drop-down list box and click Go.

Step 5  The Manager Configuration window displays and contains manager information, assistant information, and controlled lines information for the chosen user.

Tip  To view existing assistant configuration information, click the assistant name in the Associated Assistants list and click the View Details link. The Assistant Configuration information displays. To return to the manager configuration information, click the manager name in the Associated Managers list and click the View Details link.

Step 6  To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile drop-down list box. Extension mobility can optionally use device profiles. For information about using Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, see the “Extension Mobility” section on page 11-14.

Note  If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing Cisco Unified Communications Manager Assistant.

Step 7  From the Intercom Line drop-down list box, choose the intercom line appearance for the manager, if applicable.

Note  The chosen intercom line applies to the Cisco Unified Communications Manager Assistant and Cisco Unified Communications Manager intercom features.

Step 8  From the Assistant Pool drop-down list box, choose the appropriate Pool number (1 to 3).

Step 9  To assign an assistant to the manager, choose an assistant from the Available Assistants list and click the down arrow to move the chosen assistant to the Associated Assistants list.

Step 10  From the Available Lines selection box, choose a line that you want Cisco Unified Communications Manager Assistant to control and click the down arrow to make the line display in the Selected Lines selection box. Configure up to five Cisco Unified Communications Manager Assistant-controlled lines.

To remove a line from the Selected Lines selection box and from Cisco Unified Communications Manager Assistant control, click the up arrow.

Step 11  To automatically configure the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications Manager Assistant—Controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters, check the Automatic Configuration check box.

Note  Automatic Configuration for intercom applies only when using the Cisco Unified Communications Manager Assistant intercom feature for the Cisco Unified IP Phones 7940 and 7960.
Step 12  Click the **Save** button.

The update takes effect immediately.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

Upon successful completion of the automatic configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for settings to take effect.

---

**IPMA Service Restarts**

Previously, the IPMA service did not reflect changes that were made in the Unified CM Admin user interface or in the directory until the service got restarted. This was the case for:

- User name changes
- User locale changes
- User ID changes

Each time the IPMA service got restarted, all assistants got logged out.

Because of changes that were made in Cisco Unified Communications Manager, it is not necessary to restart the IPMA service in the above cases.

If a restart does occur, IPMA now preserves the authentication state and availability status of the user.

**Additional Information**

See the “Related Topics” section on page 11-44.

---

**Deleting Cisco Unified Communications Manager Assistant Information from the Manager**

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for a manager. To delete non-Cisco Unified Communications Manager Assistant information for a manager, see the “End User Configuration Settings” section in the *Cisco Unified Communications Manager Administration Guide*.

**Procedure**

**Step 1**  To search for the manager for whom you want to delete Cisco Unified Communications Manager Assistant information, choose **User Management > End User** from Cisco Unified Communications Manager Administration.

**Step 2**  From the Find and List Users window, click the **Find** button or enter the user name in the Search Options field and click the **Find** button.

A list of configured users displays.

**Step 3**  Choose the manager whose information you want to delete.

**Step 4**  From the Related Links drop-down list box, click **Manager Configuration**.

The Manager Configuration window displays and contains manager configuration information.
Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Chapter 11  Cisco Unified Communications Manager Assistant With Proxy Line Support

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Step 5  Click the Delete button.
The update takes effect immediately.

Additional Information
See the “Related Topics” section on page 11-44.

Updating the Manager Cisco Unified Communications Manager Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for a manager. To update non-Cisco Unified Communications Manager Assistant information for a manager, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1  To search for the manager for whom you want to update Cisco Unified Communications Manager Assistant information, choose User Management > End User from Cisco Unified Communications Manager Administration.

Step 2  From the Find and List Users window, click the Find button or enter the user name in the Search Options field and click the Find button.
A list of configured users displays.

Step 3  Choose the manager whose information you want to update.

Step 4  From the Related Links drop-down list box, click Manager Configuration.
The Manager Configuration window displays and contains manager configuration information.

Step 5  Update the information that you want changed such as device name, controlled lines, assistant, or intercom line appearance.

Note  When the Automatic Configuration check box is checked, the system automatically configures the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications Manager Assistant—Controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters.

Step 6  Click the Save button.
The update takes effect immediately.

Note  When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in for the changes to occur.
Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Chapter 11

Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support

Additional Information
See the “Related Topics” section on page 11-44.

Configuring Proxy, Incoming Intercom, and Primary Lines for the Assistant

Use the Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the incoming intercom call (optional)
- Primary line to make outgoing calls (optional)
- Proxy line of the assistant phone that is associated with the manager, the manager name, and the manager line. For example, the assistant phone line 3 gets used to answer manager Mary Smith phone line 2.

A proxy line specifies a phone line that appears on the assistant Cisco Unified IP Phone. Cisco Unified Communications Manager Assistant uses proxy lines to manage calls that are intended for a manager; for example, manager1. If the call-routing software determines that the call should be presented to the assistant because manager1 cannot accept the call, the call routes to the proxy line that is configured for manager1 on the assistant Cisco Unified IP Phone.

You can manually configure a line on the assistant phone to serve as the proxy line, or you can use automatic configuration to generate a DN and to add the line to the assistant phone.

For information about configuring shared and intercom lines for Cisco Unified Communications Manager Assistant with shared line mode, see the “Configuring Shared and Incoming Intercom Lines for the Assistant” section on page 12-25.

When you display Cisco Unified Communications Manager Assistant information for the assistant, the system generates DNs on the basis of Cisco IP Manager Assistant service parameter entries in the Proxy Directory Number Range and Proxy Directory Number Prefix sections. For more information about these service parameters, see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 11-24.

Perform the following procedure to configure the proxy and incoming intercom line appearances for an assistant. To configure a new user, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Tip
Before configuring the Cisco Unified Communications Manager Assistant information for an assistant, you must configure the manager information and assign an assistant to the manager. See “Configuring a Manager and Assigning an Assistant for Proxy Line Mode” section on page 11-34.

Before You Begin
If you want to automatically configure the proxy line on the assistant phone, configure the service parameters in the Proxy Directory Number Range and Proxy Directory Number Prefix sections.

Procedure

Step 1
To configure an assistant and assign proxy and incoming intercom lines, choose User Management > End User.
Step 2 To find the user that will be the assistant, click the Find button or enter the user name in the Search Options field and click the Find button.

Step 3 To display user information for the chosen assistant, click the user name. The End User Configuration window displays.

Step 4 To configure Cisco Unified Communications Manager Assistant information for the assistant, choose Assistant Configuration from the Related Links drop-down list box and click Go. The Assistant Configuration window displays.

Step 5 From the Device Name drop-down list box, choose the device name to associate with the assistant.

Step 6 From the Intercom Line drop-down list box, choose the incoming intercom line appearance for the assistant.

Step 7 From the Primary Line drop-down list box, choose the primary line appearance for the assistant.

Step 8 Use the selection boxes in the Manager Association to Assistant Line area to assign and associate manager line numbers to the assistant line numbers. In the Available Lines selection box, choose the assistant line. The word “Auto” precedes the autogenerated proxy lines. If you want Cisco Unified Communications Manager to create an autogenerated proxy line on the assistant phone, choose an autogenerated proxy line and ensure that the Automatic Configuration check box is checked.

Note The system automatically sets the softkey template as well as the calling search space and partition for existing proxy lines and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings when the Automatic Configuration check box is checked. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 9 In the Manager Names selection box, choose the manager for whom this proxy line will apply.

Step 10 In the Manager Lines selection box, choose the manager line for which this proxy line will apply.

Step 11 Click the Save button. The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Additional Information
See the “Related Topics” section on page 11-44.

Deleting the Cisco Unified Communications Manager Assistant Information from the Assistant

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for an assistant. To delete non-Cisco Unified Communications Manager Assistant information for an assistant, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to delete Cisco Unified Communications Manager Assistant information, choose User Management > End User from Cisco Unified Communications Manager Administration.
Step 2  From the Find and List Users window, click the Find button or enter the user name in the Search Options field and click the Find button.  
A list of configured users displays.

Step 3  Choose the assistant whose information you want to delete.

Step 4  From the Related Links drop-down list box, click Assistant Configuration. 
The Assistant Configuration window displays.

Step 5  Click the Delete button. 
The update takes effect immediately.

---

**Note**  
When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

---

**Additional Information**  
See the “Related Topics” section on page 11-44.

---

**Updating the Assistant Cisco Unified Communications Manager Assistant Configuration**

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for an assistant. To update non-Cisco Unified Communications Manager Assistant information for an assistant, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

**Procedure**

Step 1  To search for the assistant for whom you want to update information, choose User Management > End User from Cisco Unified Communications Manager Administration.

Step 2  From the Find and List Users window, click the Find button or enter the user name in the Search Options field and click the Find button.  
A list of configured users displays.

Step 3  Choose the assistant whose information you want to update.

Step 4  From the Related Links drop-down list box, click Assistant Configuration. 
The Assistant Configuration window displays.

Step 5  Update the information such as device name, intercom line, or manager association information that you want changed.

**Note**  
The system automatically configures the softkey template, subscription to the Cisco Unified Communications Manager Assistant phone service, calling search space and partition for Cisco Unified Communications Manager Assistant—Controlled selected lines and intercom line, and auto answer with speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters when the Automatic Configuration check box is checked.
Step 6
Click the Save button.
The update takes effect immediately.

Note
When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes can occur.

Additional Information
See the “Related Topics” section on page 11-44.

Dial Rules Configuration
The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that the assistant dials from the directory search window in the Assistant Console. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The following sections provide additional information on application dial rules:
- Application Dial Rules Configuration Design, Cisco Unified Communications Manager System Guide
- Application Dial Rules Configuration Error Checking, Cisco Unified Communications Manager System Guide

Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants
Install the assistant console application for Cisco Unified Communications Manager Assistant by accessing a URL. The administrator sends the URL, in the “Installing the Assistant Console Plug-In” section on page 11-41, to the assistant.

Note
The assistant console application installation program supports Microsoft Internet Explorer 7, Internet Explorer 8, FireFox 3.x and Safari 4.x.

Installing the Assistant Console Plug-In
The assistant console plug-in installation supports Internet Explorer 7, Internet Explorer 7, FireFox 3.x and Safari 4.x. You can install the application on a PC that runs Windows XP, Windows Vista or Apple MAC OS X.

A previous 5.x or 6.x version of the assistant console application works with Cisco Unified Communications Manager 7.1, but if you decide to install the 7.1 plug-in, you must uninstall the previous 5.x or 6.x version of the assistant console application before you install the plug-in.
Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager 7.1, you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

To uninstall previous versions of the assistant console application (6.0(1), 4.x, or any 5.x version before 5.1(3)), choose Start> ...Programs > Cisco Unified CallManager Assistant > Uninstall Assistant Console.

To uninstall a 5.1(3) or 6.1(x) assistant console application, go to the Control Panel and remove it.

Tip
The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified Communications Manager.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse to Cisco Unified Communications Manager Administration and choose Application > Plugins.

Step 2 For the Cisco Unified Communications Manager Assistant plug-in, click the Download link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click Next.

Step 5 Accept the license agreement and click Next.

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click Next.

Tip By default, the application installs in C:\Program Files\Cisco\ Unified Communications Manager Assistant Console.

Step 7 To install the application, click Next.

The installation begins.

Step 8 After the installation completes, click Finish.
Tip

To launch the assistant console, click the desktop icon or choose Cisco Unified Communications Manager Assistant > Assistant Console in the Start...Programs menu.

Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Cisco Unified Communications Manager server where the Cisco IP Manager Assistant service is activated. The first time that the assistant logs in to the console, the assistant must enter the information in the Cisco Unified Communications Manager Assistant Server Port and the Cisco Unified Communications Manager Assistant Server Hostname or IP Address fields.

Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

The Advanced tab in the Cisco Unified Communications Manager Assistant Settings window allows you to enable trace for the assistant console.

Assistant Console Dialog Options

The assistant console displays a dialog that contains the following options:

- Location to Install—The path of the directory where the assistant console software gets installed. The default specifies following path:
  
  c:\Program Files\Cisco\Cisco Unified Communications Manager Assistant Console

- Create Desktop Shortcut—Default specifies true. This parameter determines whether a shortcut is created on the assistant console.

- Create StartMenu Shortcut—Default specifies true. This parameter determines whether a shortcut is created in the Start menu (Start > Programs > Cisco Unified Communications Manager Assistant > Assistant Console).

- Install JRE—Default specifies true. This parameter determines whether JRE is installed along with assistant console. If this option is turned off, the following configuration must exist on the assistant console:
  
  - Install JRE 1.4.2_05 (international version) on the assistant console.
  - Create an environment variable—Assistant_JRE on the assistant console, which gives the path to the JRE; for example, c:\Program Files\Java\j2re1.4.2_05.

Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

https://<Cisco Unified Communications Manager Assistant server>:8443/ma/desktop/maLogin.jsp

where

Cisco Unified Communications Manager Assistant server specifies the IP address of the server on which the Cisco IP Manager Assistant service is running.

The administrator must send this URL to the manager.
Related Topics

Additional Information
See the “Related Topics” section on page 11-44.

Related Topics

- Configuration Checklist for Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-2
- Introducing Cisco Unified Communications Manager Assistant, page 11-5
- System Requirements for Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-12
- Interactions and Restrictions, page 11-13
- Installing and Activating Cisco Unified Communications Manager Assistant, page 11-17
- Configuring Cisco Unified Communications Manager Assistant with Proxy Line Support, page 11-18
- Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants, page 11-41
- Cisco Unified Communications Manager Assistant With Shared Line Support, page 12-1
- Softkey Templates, Cisco Unified Communications Manager System Guide
- End User Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Associating Devices to an End User, Cisco Unified Communications Manager Administration Guide
- Intercom, page 28-1
- Internet Protocol Version 6 (IPv6), page 29-1

Additional Cisco Documentation

- Cisco Unified Communications Manager Assistant User Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
Cisco Unified Communications Manager Assistant With Shared Line Support

The Cisco Unified Communications Manager Assistant feature enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support. The Cisco IP Manager Assistant service supports both proxy line and shared line support simultaneously in a cluster.

The feature comprises enhancements to phone capabilities for the manager and the assistant console application that are primarily used by the assistant.

Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants. To accommodate this number of users, the administrator configures up to three Cisco Unified Communications Manager Assistant applications in one Cisco Unified Communications Manager cluster and assigns managers and assistants to each instance of the application.

Cisco Unified Communications Manager users comprise managers and assistants. An assistant user handles calls on behalf of a manager. Cisco Unified Communications Manager Assistant comprises features for managers and features for assistants.

This chapter provides the following information about Cisco Unified Communications Manager Assistant:

- Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-2
- Introducing Cisco Unified Communications Manager Assistant, page 12-5
- System Requirements for Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-10
- Interactions and Restrictions, page 12-11
- Installing and Activating Cisco Unified Communications Manager Assistant, page 12-15
- Configuring Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-15
- Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants, page 12-28
- Related Topics, page 12-31
Cisco Unified Communications Manager Assistant With Shared Line Support

Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. If you configure Cisco Unified Communications Manager Assistant in shared-line mode, the manager and assistant share a directory number; for example, 8001. The assistant handles calls for a manager on the shared directory number. When a manager receives a call on 8001, both the manager phone and the assistant phone rings.

The Cisco Unified Communications Manager Assistant features that do not apply to shared-line mode include default assistant selection, assistant watch, call filtering, and divert all calls. An assistant cannot see or access these features on the Assistant Console application. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

Table 12-1 shows the steps for configuring the Cisco Unified Communications Manager Assistant with shared line support. For more information on Cisco Unified Communications Manager Assistant with shared line support, see the “Introducing Cisco Unified Communications Manager Assistant” section on page 12-5 and the “Related Topics” section on page 12-31.

Table 12-1  Cisco Unified Communications Manager Assistant Configuration Checklist with Shared Line Support

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you have not already done so, configure the phones and users and associate the devices to the users. Additionally, for shared line appearances between managers and assistants, configure the same directory number on the manager primary line and assistant secondary line, if you have not already done so.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In Cisco Unified Serviceability, activate the Cisco IP Manager Assistant service in the Service Activation window.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure Cisco IP Manager Assistant service parameters for shared line support.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>If using the Cisco Unified Communications Manager intercom feature, add the Intercom partition, Intercom calling search space, Intercom directory number, and the Intercom translation pattern.</td>
</tr>
</tbody>
</table>
### Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| **Step 5** | If multiple Cisco Unified Communications Manager Assistant pools are required to support large numbers of assistants and managers, configure the following Cisco IP Manager Assistant clusterwide service parameters:  
- Enable Multiple Active Mode  
- Pool 2 and Pool 3 Cisco IPMA Server IP Address | Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, page 12-18 |
| **Step 6** |  
- Configure the application user CAPF profile (optional).  
- Configure Cisco IP Manager Assistant service parameters for security (optional). | Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 12-16  
Security Considerations, page 12-19 |
| **Step 7** | Using the Serviceability Control Center Feature Services, stop and start the Cisco IP Manager Assistant service. | Starting the Cisco IP Manager Assistant Service, page 12-19 |
| **Step 8** | Add the appropriate Cisco Unified IP Phone phone button template. | Phone Button Template Configuration Settings, Cisco Unified Communications Manager Administration Guide |
| **Step 9** | Configure manager and assistant Cisco Unified IP Phone parameters:  
- Set up manager phone.  
- Set up assistant phone. | Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide |
| **Step 10** | Configure manager phone settings:  
- Assign the softkey template for shared line mode.  
- If using Do Not Disturb, configure the Do Not Disturb fields on the manager phone.  
- Add primary lines. (Use the same DN and partition for the assistant secondary line DN.)  
- Set up voice-mail profile on primary line.  
- Add incoming intercom line (optional).  
- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.  
- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975 add the intercom capabilities.  
- Set user locale.  
- Reset the phone.  
**Tip** To automatically configure some manager phone settings, choose the automatic configuration check box on the Manager Configuration window when you are configuring the manager. For more information, see the “Manager Phones” section on page 12-20. | Manager and Assistant Phone Configuration, page 12-19  
Phone Configuration Settings, Cisco Unified Communications Manager Administration Guide  
Tips About Deleting Phones, Cisco Unified Communications Manager Administration Guide  
Directory Number Configuration, Cisco Unified Communications Manager Administration Guide  
Do Not Disturb, page 21-1  
Intercom, page 12-14  
Intercom, page 28-1  
Configuring Speed-Dial Buttons or Abbreviated Dialing, Cisco Unified Communications Manager Administration Guide  
Tips About Resetting a Phone, Cisco Unified Communications Manager Administration Guide |
### Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>Cisco Unified Communications Manager Assistant Configuration Checklist</strong></td>
</tr>
<tr>
<td>Configure assistant phone settings:</td>
<td>Manager and Assistant Phone Configuration, page 12-19</td>
</tr>
<tr>
<td>- Assign a softkey template.</td>
<td>Phone Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>- Add an expansion module (optional).</td>
<td>Tips About Deleting Phones, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>- Assign the phone button template.</td>
<td>Directory Number Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>- Add a primary line.</td>
<td>Intercom, page 12-14</td>
</tr>
<tr>
<td>- Add shared lines for each configured manager. (Use the same DN and partition for the assistant secondary line and manager primary line.)</td>
<td>Intercom, page 28-1</td>
</tr>
<tr>
<td>- Add incoming intercom line (optional).</td>
<td>Configuring Speed-Dial Buttons or Abbreviated Dialing, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>- For Cisco Unified IP Phones 7940 and 7960, add speed dial for outgoing intercom targets.</td>
<td>Tips About Resetting a Phone, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>- For Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975, add the intercom capabilities.</td>
<td></td>
</tr>
<tr>
<td>- Set user locale.</td>
<td></td>
</tr>
<tr>
<td>- Reset the phone.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To automatically configure some assistant phone settings, choose the Automatic Configuration check box on the Assistant Configuration window when you are configuring the assistant. For more information, see the “Assistant Phones” section on page 12-21.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Configure Cisco Unified Communications Manager Assistant:</td>
</tr>
<tr>
<td>Create a new manager.</td>
<td>Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 12-22</td>
</tr>
<tr>
<td>Configure shared lines for manager.</td>
<td>Deleting Cisco Unified Communications Manager Assistant Information for the Manager, page 12-24</td>
</tr>
<tr>
<td>Assign an assistant to a manager.</td>
<td>Configuring Shared and Incoming Intercom Lines for the Assistant, page 12-25</td>
</tr>
<tr>
<td>Configure lines for the assistant.</td>
<td>Intercom, page 12-14</td>
</tr>
<tr>
<td>Configure intercom lines (optional)</td>
<td>Intercom, page 28-1</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Configure the dial rules for the assistant.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Install the Assistant Console application.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Configure the manager and assistant console applications.</td>
</tr>
</tbody>
</table>
Introducing Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant, a plug-in that allows an assistant to handle calls on behalf of a manager, intercepts manager calls and routes them appropriately. If you configure Cisco Unified Communications Manager Assistant in shared-line mode, the manager and assistant share a directory number; for example, 8001. The assistant handles calls for a manager on the shared directory number. When a manager receives a call on 8001, both the manager phone and the assistant phone rings.

The Cisco Unified Communications Manager Assistant features that do not apply to shared-line mode include default assistant selection, assistant watch, call filtering, and divert all calls. An assistant cannot see or access these features on the Assistant Console application. The assistant phone does not have the softkey for the divert all feature. The manager phone does not have the softkeys for assistant watch, call intercept, or divert all feature.

Table 12-1 shows the steps for configuring the Cisco Unified Communications Manager Assistant with shared line support. For more information on Cisco Unified Communications Manager Assistant with shared line support, see the “Related Topics” section on page 12-31.

The following sections provide information about the Cisco Unified Communications Manager Assistant feature:

- Cisco Unified Communications Manager Assistant Architecture Overview, page 12-5
- Cisco Unified Communications Manager Assistant Database Access Architecture, page 12-8
- Manager Interfaces, page 12-8
- Assistant Interfaces, page 12-8
- Softkeys, page 12-9
- Cisco Unified Communications Manager Assistant Administration Interface, page 12-9

Cisco Unified Communications Manager Assistant Architecture Overview

The Cisco Unified Communications Manager Assistant feature architecture comprises the Cisco IP Manager Assistant service, the assistant console application, and the Cisco Unified IP Phone interfaces. See Figure 12-1.

Additional Information

See the “Related Topics” section on page 12-31.
Chapter 12  Cisco Unified Communications Manager Assistant With Shared Line Support

Introducing Cisco Unified Communications Manager Assistant

Figure 12-1  Cisco Unified Communications Manager Assistant Architecture

Cisco IP Manager Assistant Service

Cisco Tomcat loads the Cisco IP Manager Assistant service, a servlet. Cisco Tomcat gets installed at Cisco Unified Communications Manager installation.

The Cisco IP Manager Assistant service gets installed on all Cisco Unified Communications Manager servers in a cluster. After installation, the administrator activates the service from Serviceability, which automatically starts Cisco Unified Communications Manager Assistant. The Cisco IP Manager Assistant service checks to see whether it is one of the Cisco Unified Communications Manager Assistant servers that is configured in the clusterwide service parameter, Cisco IPMA Server (Primary) IP Address. If it is, the Cisco IP Manager Assistant service attempts to become the active Cisco IP Manager Assistant service. Currently, a Cisco Unified Communications Manager cluster supports only one active Cisco IP Manager Assistant service.

The Cisco IP Manager Assistant service performs the following tasks:

- Hosts the HTTP services that run on the manager phone.
- Hosts the web pages that the manager uses for configuration.
- Communicates to a Cisco Unified Communications Manager cluster through the Cisco CTIManager for third-party call control. Cisco Unified Communications Manager Assistant requires only one CTI connection for all users in a cluster.
- Accesses data from the database.
- Supports the Assistant Console application.

Cisco Unified Communications Manager supports redundancy of the Cisco IP Manager Assistant service. To achieve redundancy, you must configure a second Cisco IP Manager Assistant service in the same cluster.
Cisco Unified Communications Manager Assistant implements redundancy by using an active/standby server model. At any time, only one Cisco Unified Communications Manager Assistant server remains active and servicing all assistant console applications and phones. The other server stays in a standby mode and will detect failures on the active server. When the backup server detects a failure, it takes over and becomes the active server. All connections that were active get restored on the new server, and service continues uninterrupted to the users.

If the active server fails, the Assistant Console application fails over automatically to the backup server. The Cisco IPMA Assistant Console Heartbeat Interval service parameter (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16) determines the time that the application takes to detect failure. A shorter heartbeat interval leads to faster failover. See Figure 12-2.

The Cisco IP Manager Assistant service includes built-in security to help prevent unauthorized access to its services. The user ID and password that are collected at the assistant console get encrypted before they are sent over the network. The Assistant Console blocks nonauthorized users who are posing as assistants.

**Assistant Console Interface**

Cisco Unified Communications Manager Assistant supports the following assistant console interfaces for managers and assistants:

- Assistant Console (used for call control, log on, assistant preferences, monitoring managers call activity, keyboard shortcuts)
- Manager configuration (used for configuring the immediate divert target)

Administrators use Cisco Unified Communications Manager Administration, End User Configuration, to configure Cisco Unified Communications Manager Assistant for managers and assistants. See “Cisco Unified Communications Manager Assistant Administration Interface” section on page 12-9.
Cisco Unified Communications Manager makes the Cisco Unified Communications Manager Assistant manager features available through the Cisco Unified IP Phone. Use a browser to access Manager configuration. Assistants use the Cisco Unified IP Phone and the assistant console application. See “Manager Interfaces” section on page 12-8 and “Assistant Interfaces” section on page 12-8.

For more information about how to use the assistant console features, see the Cisco Unified Communications Manager Assistant User Guide.

Cisco Unified IP Phone Interface

Assistants and managers use softkeys to access Cisco Unified Communications Manager Assistant features. For more information about how to use the Cisco Unified Communications Manager Assistant phone features, see the Cisco Unified Communications Manager Assistant User Guide.

See “Manager Interfaces” section on page 12-8 and “Assistant Interfaces” section on page 12-8.

Cisco Unified Communications Manager Assistant Database Access Architecture

The database stores all Cisco Unified Communications Manager Assistant configuration information. When the manager or assistant logs in, the Cisco IP Manager Assistant service retrieves all data that is related to the manager or assistant from the database and stores it in memory.

Manager Interfaces

The manager phone makes available the manager features with the exception of Manager Configuration. Cisco Unified Communications Manager Assistant automatically logs a manager into the Cisco IP Manager Assistant service when the Cisco IP Manager Assistant service starts.

The manager accesses the Cisco Unified Communications Manager Assistant features Assistant Watch, Intercept Call, and Transfer to Voice Mail from the Cisco Unified IP Phone softkeys.

Note

Managers also have access to Cisco Unified Communications Manager features such as Do Not Disturb and i-Divert.

The state of the Do Not Disturb feature displays in the Status Window on the Cisco Unified IP Phone. See the Cisco Unified Communications Manager Assistant User Guide for more information.

Assistant Interfaces

The assistant accesses the Cisco Unified Communications Manager Assistant features by using the Assistant Console application and the Cisco Unified IP Phone. The Assistant Console, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log on and log off, to set up assistant preferences, and to display the manager configuration window that is used to configure manager preferences.

The Assistant Console displays the assistant lines and the manager shared lines. Assistants access the shared lines to manage calls that are intended for a manager.
You can access Intercom and Distinctive Ringing on the assistant Cisco Unified IP Phone. When the assistant logs in from the Assistant Console, the softkeys Redirect and Transfer to Voice Mail become active for the shared lines. See the *Cisco Unified Communications Manager Assistant User Guide* for more information.

### Softkeys

The Cisco Unified Communications Manager Assistant feature supports softkeys such as Redirect, Transfer to Voice Mail, and Do Not Disturb on the Cisco Unified IP Phone. Softkeys only appear in their appropriate call state; for example, Transfer to Voice Mail does not appear if no active calls exist.

Cisco Unified Communications Manager Assistant supports the following softkey templates:

- Standard Manager—Supports manager for proxy mode
- Standard Shared Mode Manager—Supports manager for shared mode
- Standard Assistant—Supports assistant in proxy or shared mode

Additionally, the system makes call-processing (such as hold and dial) softkeys available with the Standard User template. The administrator configures the appropriate softkey template for the devices that managers and assistants use.

**Note**

The default process assigns call-processing softkey templates to devices.

Administrators can create custom softkey templates in addition to using the standard softkey templates that are included in Cisco Unified Communications Manager. Use Softkey Template configuration in Cisco Unified Communications Manager Administration to associate softkey templates with Cisco Unified Communications Manager Assistant devices and to create custom softkey templates. See [Softkey Template Configuration](#) in the *Cisco Unified Communications Manager Administration Guide*.

### Cisco Unified Communications Manager Assistant Administration Interface

The administrator uses the End User Configuration window of Cisco Unified Communications Manager Administration to configure the manager and assistant. The administrator chooses the device for the manager and assistant and optionally chooses an intercom line for the manager and assistant. The administrator sets up the shared line for the manager, which gets configured for the assistant.

See the “Manager and Assistant Configuration” section on page 12-21.
System Requirements for Cisco Unified Communications Manager Assistant with Shared Line Support

Cisco Unified Communications Manager Assistant with shared line support requires the following software components to operate:

- Cisco Unified Communications Manager
- Supported Browsers and platform:
  - Cisco Unified Communications Manager Assistant administration (using Cisco Unified Communications Manager Administration) and the Assistant Console are supported on Microsoft Internet Explorer (IE) 5.5 or later, Firefox 3.x or later, and Safari 4.x or later. (See the “Interactions and Restrictions” section on page 12-11 for more information.).
  - On a computer running Microsoft Windows 2000 or later, a customer can open one of the browsers specified above.
- Cisco Unified Communications Manager Bulk Administration Tool (BAT) if bulk adding of managers and assistants is planned.

Because Cisco Unified Communications Manager Assistant installs automatically on the same server with Cisco Unified Communications Manager, an additional server is not required.

To determine which Cisco Unified IP Phones support Cisco Unified Communications Manager Assistant, see the “Devices That Support Cisco Unified Communications Manager Assistant” section on page 12-10.

Devices That Support Cisco Unified Communications Manager Assistant

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support Cisco Unified Communications Manager Assistant. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.
2. Click System Reports in the navigation bar.
3. In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.
4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.
5. To generate a report of all IP Phones that support Cisco Unified Communications Manager Assistant, choose these settings from the respective drop-down list boxes and click the Submit button:
   - Product: All
Feature: IPMA

The List Features pane displays a list of all devices that support the Cisco Unified Communications Manager Assistant feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco Unified Communications Manager Assistant:

- Interactions, page 12-11
- Restrictions, page 12-14

Interactions

The following sections describe how Cisco Unified Communications Manager Assistant interacts with Cisco Unified Communications Manager applications:

- Bulk Administration Tool, page 12-11
- Calling Party Normalization, page 12-11
- Extension Mobility, page 12-12
- Internet Protocol Version 6 (IPv6), page 12-12
- Reporting Tools, page 12-12
- Multilevel Precedence and Preemption (MLPP), page 12-13
- Intercom, page 12-14

Bulk Administration Tool

The administrator can use the Bulk Administration Tool (BAT) to add many users (managers and assistants) at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

The BAT templates that the Cisco Unified Communications Manager Assistant Configuration Wizard creates for Cisco Unified IP Phones support only the Cisco Unified Communications Manager intercom lines.

Additional Information

See the “Related Topics” section on page 12-31.

Calling Party Normalization

Cisco Unified Communications Manager Assistant automatically supports localized and globalized calls if you configure the calling party normalization feature. Cisco Unified Communications Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming
call to the manager, Cisco Unified Communications Manager Assistant can display localized and
globalized calling party numbers when filter pattern matching occurs. For information on configuring
calling party normalization, see the “Calling Party Normalization” section on page 8-1.

Extension Mobility

A manager who uses the Cisco Extension Mobility feature can simultaneously use Cisco Unified
Communications Manager Assistant. The manager logs into the Cisco Unified IP Phone by using
extension mobility, and Cisco IP Manager Assistant service automatically gets enabled on that phone.
The manager can then access the Cisco Unified Communications Manager Assistant features.

To have access to Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, the
administrator checks the Mobile Manager check box in the Manager Configuration window in Cisco
Unified Communications Manager Administration (accessed from the End User Configuration window).
See the “Configuring a Manager and Assigning an Assistant for Shared Line Mode” section on
page 12-22. For more information about configuring device profiles, see “Device Profile Configuration
Settings” in the Cisco Unified Communications Manager Administration Guide. For more information
about Cisco Extension Mobility, see Chapter 9, “Cisco Extension Mobility.”

Internet Protocol Version 6 (IPv6)

Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with
an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you
want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you
configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. For more information
on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

Reporting Tools

Cisco Unified Communications Manager Assistant provides statistical information in the CDR Analysis
and Reporting (CAR) tool and provides a summary of changes to configurations in a change log. The
following sections describe these reporting tools.

CDR Analysis and Reporting

Cisco Unified Communications Manager Assistant supports call-completion statistics for managers and
assistants and inventory reporting for managers and assistants. The CDR Analysis and Reporting (CAR)
tool supports call-completion statistics. Cisco Unified Serviceability supports inventory reporting. See
the Cisco Unified Communications Manager System Guide, the Cisco Unified Serviceability
Administration Guide, and the Cisco Unified Communications Manager CDR Analysis and Reporting
Administration Guide for more information.

Unified CM AssistantChangeLog*.txt

The administrator can view a summary of changes that are made to the Manager or Assistant
Configurations. A manager can change defaults by accessing the Manager Configuration from a URL.
An assistant can change the manager defaults from the Assistant Console.

Note

See the Cisco Unified Communications Manager Assistant User Guide for information about the URL
and Manager Configuration.
When changes are made, the information gets sent to a log file that is called ipma_changeLogxxx.log. The log file resides on the server that runs the Cisco IP Manager Assistant service. Use the following command to obtain the log file:

```
file get activelog tomcat/logs/ipma/log4j/
```

The administrator can download this file from the server by using the Trace Collection Tool in the Cisco Unified Real Time Monitoring Tool (RTMT). See the Cisco Unified Real Time Monitoring Tool Administration Guide for more information.

The log file contains the following fields:
- **LineNumber**—The line in the log file with information about changes
- **TimeStamp**—The time that the configuration changed
- **for Manager/Assistant**—Designation of whether the change is for the manager or the assistant
- **for Userid**—The userid of the manager or assistant that is being changed
- **by Manager/Assistant**—Designation of whether the change was made by the manager or the assistant
- **by Userid**—The userid of the manager or assistant who made the change
- **Parameter Name**—What changed; for example, divert target number
- **Old Value**—The value of the information before the change
- **New Value**—The value of the information after the change

Because the information in the log file is comma delimited, the administrator can open the log file by using a spreadsheet application such as Microsoft Excel. Use the following procedure to save the log file contents to the Microsoft Excel application.

**Procedure**

1. **Step 1** Start the Microsoft Excel application.
2. **Step 2** Choose **File > Open** to open the Unified CM Assistant.txt file.
3. **Step 3** Choose the Original data type, file type as Delimited and click **Next**.
4. **Step 4** Choose Delimiters as Comma and click **Next**.
5. **Step 5** When complete, click **Finish**.

### Multilevel Precedence and Preemption (MLPP)

The following points describe the interactions between Cisco Unified Communications Manager Assistant with shared line support and MLPP:

- The system preserves call precedence in the handling of calls by Cisco Unified Communications Manager Assistant. For example, when an assistant diverts a call, the system preserves the precedence of the call.
- Because Cisco Unified Communications Manager Assistant does not have knowledge of the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.
Intercom

Cisco Unified Communications Manager Assistant supports the following two types of intercom:

- Cisco Unified Communications Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). This intercom feature gets configured by using the DN configuration and end user (manager and assistant) configuration windows.
- Cisco Unified Communications Manager intercom (used with Cisco Unified IP Phones 7942, 7945, 7962, 7965, 7975). This intercom feature gets configured by using the intercom partition, intercom calling search space, intercom directory number, intercom translation pattern, DN, and end user (manager and assistant) configuration windows.

Restrictions

The following restrictions apply to Cisco Unified Communications Manager Assistant:

- Cisco Unified Communications Manager Assistant supports SIP on Cisco Unified IP Phones 7900 series except the Cisco Unified IP Phone 7940 and 7960.
- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants by configuring multiple Cisco IP Manager Assistant servers (pools). When multiple pools are enabled, a manager and all configured assistants for that manager should belong to the same pool.
- One manager can have up to 10 assigned assistants.
- One assistant can support up to 33 managers (if each manager has one Cisco Unified Communications Manager-controlled line).
- Cisco Unified Communications Manager Assistant supports up to 3500 managers and 3500 assistants per Cisco Unified Communications Manager cluster when you are using the MCS 7845 server.
- The Assistant Console does not support hunt groups/queues.
- The Assistant Console does not support record and monitoring.
- The Assistant Console does not support on-hook transfer (the ability to transfer a call by pressing the Transfer softkey and going on hook to complete the transfer).
- The Assistant Console does not support the one-touch Call Pickup feature.
- Cisco Unified IP Phones 7940, 7942, and 7945 support only two lines or speed-dial buttons.
- When an upgrade to Cisco Unified Communications Manager Release 8.0(2) (or higher) occurs, existing Cisco Unified Communications Manager Assistant users that use the incoming intercom line do not get upgraded automatically to the Cisco Unified Communications Manager Intercom feature.
- The system does not support calls between the Cisco Unified Communications Manager Intercom feature and regular lines (which may be configured as Cisco Unified Communications Manager Assistant Intercom lines).
- Cisco Unified IP Phones 7960 and 7940 support only the Cisco Unified Communications Manager Assistant Intercom lines feature. Cisco Unified IP Phones 7900 (except 7940 and 7960) support only the Cisco Unified Communications Manager intercom feature.
- To install the Assistant Console application on a computer with Microsoft Internet Explorer 7 (or later) on Windows XP, install the Microsoft Java Virtual Machine (JVM) with Windows XP Service Pack 1 before the Assistant Console installation.
Installing and Activating Cisco Unified Communications Manager Assistant

Cisco Tomcat loads the Cisco Unified Communications Manager Assistant, a servlet. Cisco Tomcat gets installed and started at Cisco Unified Communications Manager installation. For more information, see the “Cisco IP Manager Assistant Service” section on page 12-6.

The administrator performs the following three steps after installation to make Cisco Unified Communications Manager Assistant available for system use:

1. Use Cisco Unified Serviceability Service Activation, located on the Tools menu, to activate the Cisco IP Manager Assistant service. See the Cisco Unified Serviceability Administration Guide.

2. Configure the applicable service parameters for the Cisco IP Manager Assistant service. See the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16.

3. Use Serviceability Control Center Feature Service to stop and start the Cisco IP Manager Assistant service. See the “Starting the Cisco IP Manager Assistant Service” section on page 12-19.

Note
If the managers and assistants will require Cisco Unified Communications Manager Assistant features to display (on the phone and assistant console) in any language other than English, verify that the locale installer is installed before configuring Cisco Unified Communications Manager Assistant. See the Cisco Unified Communications Operating System Administration Guide.

Configuring Cisco Unified Communications Manager Assistant with Shared Line Support

For successful configuration of Cisco Unified Communications Manager Assistant, review the steps in the configuration checklist, perform the user and device configuration requirements, and configure the managers and assistants.

Note
Cisco Unified Communications Manager Assistant with shared line support coexists in the same Cisco Unified Communications Manager cluster with Cisco Unified Communications Manager Assistant with proxy line support. For configuration information about proxy line support, see the “Cisco Unified Communications Manager Assistant With Proxy Line Support” section on page 11-1.

The following sections provide configuration information:

- Setting the Service Parameters for Cisco Unified Communications Manager Assistant, page 12-16
- Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability, page 12-18
- Security Considerations, page 12-19
- Starting the Cisco IP Manager Assistant Service, page 12-19
- Manager and Assistant Phone Configuration, page 12-19
- Manager and Assistant Configuration, page 12-21
Tip

Before you configure Cisco Unified Communications Manager Assistant with shared line support, review the “Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support” section on page 12-2.

Setting the Service Parameters for Cisco Unified Communications Manager Assistant

Service Parameters for the Cisco IP Manager Assistant service comprise three categories: general, clusterwide, and clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants. Specify clusterwide parameters once for all Cisco IP Manager Assistant services. Specify general parameters for each Cisco IP Manager Assistant service that is installed.

Set the Cisco IP Manager Assistant service parameters by using Cisco Unified Communications Manager Administration to access the service parameters (System > Service Parameters). Choose the server where the Cisco Unified Communications Manager Assistant application resides and then choose the Cisco IP Manager Assistant service.

Cisco IP Manager Assistant includes the following service parameters that must be configured:

- **Clusterwide Parameters That Apply to All Servers**
  - Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address. To avoid potential high CPU usage, enter the address of the local CTIManager server where the IPMA process is running when you configure the Cisco IP Manager Assistant CTIManager (Primary) IP Address service parameter.
  - Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Cisco IPMA Server Port—Default specifies Port 2912.
  - Cisco IPMA Assistant Console Heartbeat Interval—Default specifies 30 seconds. This interval timer specifies how long it takes for the failover to occur on the assistant console.
  - Cisco IPMA Assistant Console Request Timeout—Default specifies 30 seconds.
  - Cisco IPMA RNA Forward Calls—Default specifies False. This service parameter does not apply to shared line support.
  - Cisco IPMA RNA Timeout—Default specifies 10 seconds. This service parameter does not apply to shared line support.
  - CTIManager Connection Security Flag has the following two options:
    - Nonsecure—The security mode specifies nonsecure.
    - Use Cluster Default—Cisco IP Manager Assistant service fetches the security mode for the cluster. If the cluster security mode is detected as mixed, Cisco Unified Communications Manager Assistant will open a secure connection to CTI Manager by using the Application CAPF profile. To make the secure connection succeed, configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” parameters.
Configuring Cisco Unified Communications Manager Assistant with Shared Line Support

• Advanced Clusterwide
  - Enable Multiple Active Mode—The default specifies False. When this parameter is set to True, the administrator can configure up to 7000 managers and assistants by using multiple pools.
  - Pool 2: Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.
  - Pool 2: Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Pool 3: Cisco IPMA Server (Primary) IP Address—No default. Administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool 3: Cisco IPMA Server (Backup) IP Address—No default. Administrator must manually enter this IP address. Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.</td>
</tr>
</tbody>
</table>

• Cisco IPMA Service Parameters for each server
  - CTIManager (Primary) IP Address—No default. Enter the IP address of the primary CTIManager that will be used for call control.
  - CTIManager (Backup) IP Address—No default. Administrator must manually enter this IP address.
  - Route Point Device Name for Proxy Mode—Not applicable for shared line support.
  - CAPF Profile Instance Id for Secure Connection to CTIManager—This service parameter specifies the Instance Id of the Application CAPF Profile for the Application User IPMASecureSysUser that this Cisco Unified Communications Manager Assistant server will use to open a secure connection to CTIManager. You must configure this parameter if CTIManager Connection Security Flag is enabled.

Cisco Unified Communications Manager Assistant includes the following clusterwide parameters that must be configured if you want to use the Cisco Unified Communications Manager Assistant automatic configuration for managers and assistants:

• Clusterwide Parameters for Softkey Templates
  - Assistant Softkey Template—Default specifies Standard Assistant softkey template. This parameter specifies the softkey template that is assigned to the assistant device during assistant automatic configuration.
  - Manager Softkey Template for Proxy Mode—This service parameter does not apply to shared line support.
  - Manager Softkey Template for Shared Mode—Default specifies Standard Shared Mode Manager. Set this parameter to specify the shared mode softkey template that is assigned to the manager device during manager automatic configuration.

• IPMA Device Configuration Defaults for Proxy Mode—These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.

• Proxy Directory Number Range for Proxy Mode—These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.

• Proxy Directory Number Prefix for Proxy Mode—These parameters do not apply for Cisco Unified Communications Manager Assistant with shared line support.
Configuring Multiple Servers for Cisco Unified Communications Manager Assistant Scalability

Cisco Unified Communications Manager supports up to 3500 managers and 3500 assistants for a total of 7000 users. To support 7000 users, the administrator must configure multiple active Cisco IP Manager Assistant servers by enabling and setting service parameters. Administrators can configure up to three active Cisco IP Manager Assistant servers, with each managing up to 2500 pairs of managers and assistants. Each server can also have a backup server. Configure the Cisco IP Manager Assistant servers by using the Advanced Service Parameters, Enable Multiple Active Mode, Pool 2: Cisco IPMA Server, and Pool3: Cisco IPMA Server. See the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16 for more information. See Figure 12-3.

**Figure 12-3 Scalability Architecture**

1. Activate IPMA service (see the “Installing and Activating Cisco Unified Communications Manager Assistant” section on page 12-15)
2. Enable multiple active mode (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16)
3. Provide IP addresses for multiple pools (see the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16)
4. Add pool to the manager/assistant from the End User Configuration window (see the “Configuring a Manager and Assigning an Assistant for Shared Line Mode” section on page 12-22)

Migration Considerations
If you are migrating from a release previous to Cisco Unified Communications Manager Release 8.0(2), all managers and assistants will get migrated to Pool 1 (the default).

Security Considerations
Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection).

The administrator must configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node) by choosing User Management > Application User CAPF Profile. From the Application User drop-down list box that is on the Application User CAPF Profile Configuration window, the administrator chooses IPMASecureSysUser.

For more information about configuring security for Cisco Unified Communications Manager Assistant, see the information on the CTIManager Connection Security Flag and the CAPF Profile Instance Id for Secure Connection to CTIManager service parameters in the “Setting the Service Parameters for Cisco Unified Communications Manager Assistant” section on page 12-16.

The Cisco Unified Communications Manager Security Guide provides detailed security configuration procedures for CTI applications.

Starting the Cisco IP Manager Assistant Service
The Cisco IP Manager Assistant service runs as an application on Cisco Tomcat. To start or stop the Cisco IP Manager Assistant service, use the Serviceability Control Center Feature Services window.

Manager and Assistant Phone Configuration
You must configure and associate devices for each Cisco Unified Communications Manager Assistant manager and assistant. Before you begin, complete the following tasks, depending on the phone type.

Cisco Unified IP Phone 7940, 7942, 7945, 7960, 7962, 7965, and 7975 (SCCP and SIP)
- Add a Cisco Unified IP Phone for each manager and assistant that will be using Cisco Unified Communications Manager Assistant. To add these phones, use one of the following methods:
  - Manually (Device > Phone)
  - Auto registration
  - BAT
- Assign the Standard Assistant or Standard Shared Mode Manager softkey template.

Cisco Unified IP Phone 7940
You can use the Cisco Unified IP Phone 7940 for Cisco Unified Communications Manager Assistant, but certain restrictions apply:
- Add a Cisco Unified IP Phone 7940 for each manager with the following items configured:
  - Two lines, one for the primary line and one for the intercom
Chapter 12  Cisco Unified Communications Manager Assistant With Shared Line Support

Configuring Cisco Unified Communications Manager Assistant with Shared Line Support

- Softkey template for manager with shared line support
- Add a Cisco Unified IP Phone 7940 for each assistant with the following items configured:
  - Two lines, one for the primary line and one for the intercom
  - Softkey template for assistant

---

**Note**  Cisco recommends the Cisco Unified IP Phones 7960, 7962, 7965, and 7975 because they provide more functionality.

---

**Note**  Cisco Unified IP Phone 7940/60 supports only the Cisco Unified Communications Manager Assistant intercom feature.

After you complete these tasks, configure the phones as described in the following sections:
- Manager Phones, page 12-20
- Assistant Phones, page 12-21
- Nonmanager and Nonassistant Phones, page 12-21

Manager Phones

The following section describes the Cisco Unified Communications Manager Assistant requirements and tips for configuring a manager phone.

Manager Phone Configuration

Configure the manager Cisco Unified IP Phones with the following settings:
- Standard Shared Mode Manager softkey template
- Primary line
- Additional lines for shared line support (optional)
- Voice-mail profile on primary line
- If using the Cisco Unified IP Phone 7900 series, except Cisco Unified IP Phone 7940 or 7960, configure the intercom feature
- If using the Cisco Unified IP Phone 7940 or 7960, configure the incoming intercom line to support the auto answer with speakerphone or headset option
- If using the Cisco Unified IP Phone 7940 or 7960, configure the speed dial for outgoing intercom targets.
- User locale

You can automate some of these settings by choosing the Automatic Configuration check box on the End User Configuration window when you configure the manager. For step-by-step instructions, see the “Configuring a Manager and Assigning an Assistant for Shared Line Mode” section on page 12-22.

Automatic Configuration sets the following items for the manager device or device profile:
- Softkey template
- Auto answer with speakerphone for intercom line (applies only to Cisco Unified IP Phone 7940 and 7960)
Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940. For more information, see the “Cisco Unified IP Phone 7940” section on page 12-19.

Assistant Phones

The following section describes the requirements for configuring an assistant phone and provides tips on configuring an assistant phone. For step-by-step instructions, see the “Configuring Shared and Incoming Intercom Lines for the Assistant” section on page 12-25.

Assistant Phone Configuration

Configure the assistant Cisco Unified IP Phones with the following settings:

- Standard Assistant softkey template (must include the Redirect and Transfer to Voice Mail softkeys)
- Default 14-button expansion module (optional)
- Primary line
- Shared lines for each configured manager (Use the same DN and partition as the manager primary line.)
- Incoming intercom line to support the auto answer with speakerphone or headset option (applies only to Cisco Unified IP Phone 7940 and 7960)
- Speed dial to incoming intercom line for each configured manager (applies only to Cisco Unified IP Phone 7940 and 7960)
- User locale

Cisco Unified Communications Manager Assistant supports the Cisco Unified IP Phone 7940. For more information, see the “Cisco Unified IP Phone 7940” section on page 12-19.

Nonmanager and Nonassistant Phones

In addition to configuring manager and assistant devices, configure all other users in the Cisco Unified Communications Manager cluster. Proper configuration allows managers and assistants to make calls to and receive calls from all other users in the cluster.

Manager and Assistant Configuration

From the Cisco Unified Communications Manager End User Configuration window, configure the settings for the managers and assistants who use the Cisco Unified Communications Manager Assistant feature. From this window, perform the following functions:

- Choose manager and assistant devices.
- Automatically configure a manager or assistant device, if desired.
- From the Manager Configuration or Assistant Configuration window that is accessed from the End User Configuration window, configure the following settings:
  - Set up primary and incoming intercom lines for intercom capability. For example, extension 3102 serves as the intercom line for the manager. This line will receive intercom calls from the assistant. The assistant line 1 (1102) and line 2 (1103) display on the console, and the assistant answers them.
Note
The intercom line that you choose will be the one that you created by using the Cisco Unified Communications Manager intercom feature (applicable only to Cisco Unified IP Phones 7942, 7945, 7962, 7965, and 7975) or by using speed dials (applicable only to Cisco Unified IP Phones 7940 and 7960).

- Configure assistants for managers.

Note
When the shared lines for the manager and assistant are configured (using the Directory Number Configuration window in Cisco Unified Communications Manager Administration), the assistant configuration gets updated appropriately.

- Choose the local language in which the End User Configuration window displays.

The following sections provide details about configuring the manager and assistant settings:
- Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 12-22
- Deleting Cisco Unified Communications Manager Assistant Information for the Manager, page 12-24
- Deleting the Cisco Unified Communications Manager Assistant Information for the Assistant, page 12-27
- Configuring Shared and Incoming Intercom Lines for the Assistant, page 12-25
- Intercom, page 28-1

### Configuring a Manager and Assigning an Assistant for Shared Line Mode

Perform the following procedure to configure a Cisco Unified Communications Manager Assistant manager and assign an assistant to the manager. To configure a new user and associate the device to the user, see “End User Configuration Settings” in the Cisco Unified Communications Manager Administration Guide. To configure the same directory number for the manager primary line and assistant secondary line, see “Directory Number Configuration” in the Cisco Unified Communications Manager Administration Guide.

Tip
Configure manager information before configuring Cisco Unified Communications Manager Assistant information for an assistant.

### Procedure

**Step 1**
To configure the manager and to assign an assistant to an existing user, choose User Management > End User. From the Find and List Users window, click the Find button. The window displays all of the end users that are configured in Cisco Unified Communications Manager.

**Step 2**
To display user information for the chosen manager, click the user name. The End User Configuration window displays.

**Step 3**
To configure Cisco Unified Communications Manager Assistant information for the manager, choose Manager Configuration from the Related Links drop-down list box and click Go.

**Step 4**
The Manager Configuration window displays and contains manager information, assistant information, and controlled lines information.
Step 5 To automatically configure the softkey template and auto answer with speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters, check the Automatic Configuration check box.

**Note** Automatic Configuration for intercom applies only when the Cisco Unified Communications Manager Assistant intercom feature is used for the Cisco Unified IP Phones 7940 and 7960.

Step 6 Click the Uses Shared Lines check box.

Step 7 To associate a device name or device profile with a manager, choose the device name or device profile from the Device Name/Profile drop-down list box. (Extension mobility uses device profiles.) For information about using Cisco Extension Mobility with Cisco Unified Communications Manager Assistant, see the “Extension Mobility” section on page 12-12.

**Note** If the manager telecommutes, click the Mobile Manager check box and optionally choose Device Profile. When Device Profile is chosen, the manager must log on to the phone by using extension mobility before accessing Cisco Unified Communications Manager Assistant.

Step 8 From the Intercom Line drop-down list box, choose the intercom line appearance for the manager, if applicable.

**Note** The chosen intercom line applies to the Cisco Unified Communications Manager Assistant and Cisco Unified Communications Manager intercom features.

Step 9 If applicable, from the Assistant Pool drop-down list box, choose the appropriate Pool number (1 to 3).

Step 10 To assign an assistant to the manager, choose the name of the assistant from the Available Assistants list and move it to the Associated Assistants list box by clicking the down arrow.

**Tip** You can go to the Assistant Configuration window by highlighting the assistant name and clicking the View Details link.

Step 11 To configure the Cisco Unified Communications Manager Assistant controlled lines, choose the appropriate line from the Available Lines list box and move it to the Selected Lines list box by clicking the down arrow.

**Note** Ensure the controlled line is always the shared line DN.

To remove a line from the Selected Lines selection box and from Cisco Unified Communications Manager Assistant control, highlight the line and click the up arrow.

Step 12 Click the Save button.

If you checked the Automatic Configuration check box and the service parameters are invalid, a message displays.

Upon successful completion of the automatic configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for settings to take effect.
Deleting Cisco Unified Communications Manager Assistant Information for the Manager

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for a manager. To delete non-Cisco Unified Communications Manager Assistant information for a manager, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

**Step 1**
To search for the manager for whom you want to delete Cisco Unified Communications Manager Assistant information, choose **User Management > End User** from Cisco Unified Communications Manager Administration.

**Step 2**
From the Find and List Users window, click the **Find** button. The window displays all of the end users that are configured in Cisco Unified Communications Manager.

**Step 3**
From the Find and List Users window, choose the manager whose information you want to delete. The End User Configuration window displays.

**Step 4**
From the Related Links drop-down list box, choose **Manager Configuration** and click **Go**. The Manager Configuration window displays for the user that you chose.

**Step 5**
Click the **Delete** button.
The update takes effect immediately.

Additional Information
See the “Related Topics” section on page 12-31.

Updating the Manager Cisco Unified Communications Manager Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for a manager. To update non-Cisco Unified Communications Manager Assistant information for a manager, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

**Step 1**
To search for the manager for whom you want to update information, choose **User Management > End User** from Cisco Unified Communications Manager Administration.

**Step 2**
From the Find and List Users window, click the **Find** button. The window displays all the end users that are configured in Cisco Unified Communications Manager.
Step 3  From the Find and List Users window, choose the manager whose information you want to update. The End User Configuration window displays.

Step 4  From the Related Links drop-down list box, choose Manager Configuration and click Go. The Manager Configuration window displays for the user that you chose.

Step 5  Update the information that you want changed such as device name, controlled lines, or intercom line appearance.

Step 6  Click the Save button.

The update takes effect immediately.

Note  The system automatically configures the softkey template and auto answer with speakerphone for intercom line for the manager phone on the basis of the Cisco IP Manager Assistant service parameters when the Automatic Configuration check box is checked.

Note  When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in for the changes to occur.

Additional Information  See the “Related Topics” section on page 12-31.

Configuring Shared and Incoming Intercom Lines for the Assistant

Use the Assistant Configuration of the End User Configuration window to configure the following items:

- Device name of the assistant phone
- Intercom line that the assistant uses to answer the manager calls (optional)
- Shared line of the manager to which the assistant phone gets associated (this gets done automatically when the manager and assistant share the same DN).

Administrators can set up one or more lines with a shared line appearance. The Cisco Unified Communications Manager system considers a directory number to be a shared line if it appears on more than one device in the same partition.

In a shared line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone.

Perform the following procedure to configure the manager shared line and incoming intercom line appearances for an assistant. To configure a new user and associate devices, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Tip  Before configuring the Cisco Unified Communications Manager Assistant information for an assistant, you must configure the manager information and assign an assistant to the manager. See “Configuring a Manager and Assigning an Assistant for Shared Line Mode” section on page 12-22.
Chapter 12  Cisco Unified Communications Manager Assistant With Shared Line Support

Configuring Cisco Unified Communications Manager Assistant with Shared Line Support

Procedure

Step 1  To search for the assistant for whom you want to configure Cisco Unified Communications Manager Assistant information, choose User Management > End User from Cisco Unified Communications Manager Administration.

Step 2  From the Find and List Users window, click the Find button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3  To display user information for the chosen assistant, click the user name. The End User Configuration window displays.

Step 4  To configure information for the assistant, choose Assistant Configuration from the Related Links drop-down list box and click Go. The Assistant Configuration window displays for the user that you chose.

Note  The system automatically sets the softkey template and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings when the Automatic Configuration check box is checked. Additionally, the system sets auto answer with speakerphone for intercom line.

Step 5  From the Device Name drop-down list box, choose the device name to associate with the assistant.

Step 6  From the Intercom Line drop-down list box, choose the incoming intercom line appearance for the assistant.

Step 7  From the Primary Line drop-down list box, choose the primary line for the assistant. In the Associated Manager selection list box, the name of the previously configured manager displays.

Tip  To view existing manager configuration information, highlight the manager name in the Associated Managers list and click the View Details link. The Manager Configuration window displays. To return to the Assistant Configuration window, highlight the assistant name and click the View Details link on the Manager Configuration window.

Step 8  To associate the manager line to the assistant line, perform the following steps from the Manager Association to the Assistant Line selection box:

a. In the Available Lines drop-down list box, choose the assistant line that will be associated with the manager line.

b. In the Manager Names drop-down list box, choose the preconfigured manager name with which the assistant is associated.

c. In the Manager Lines drop-down list box, choose the manager line that will be associated with the assistant line.

Step 9  Click the Save button. The update takes effect immediately. If you chose automatic configuration, the assistant device automatically resets.

Additional Information

See the “Related Topics” section on page 12-31.
Deleting the Cisco Unified Communications Manager Assistant Information for the Assistant

Perform the following procedure to delete Cisco Unified Communications Manager Assistant information for an assistant. To delete non-Cisco Unified Communications Manager Assistant information for an assistant, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to delete information, choose User Management > End User from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the Find button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the assistant whose information you want to delete. The End User Configuration window displays.

Step 4 From the Related Links drop-down list box, choose Assistant Configuration and click Go. The Assistant Configuration window displays for the user that you chose.

Step 5 Click the Delete button.

The update takes effect immediately.

Note When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Additional Information

See the “Related Topics” section on page 12-31.

Updating the Assistant Cisco Unified Communications Manager Assistant Configuration

Perform the following procedure to update Cisco Unified Communications Manager Assistant information for an assistant. To update non-Cisco Unified Communications Manager Assistant information for an assistant, see the “End User Configuration Settings” section in the Cisco Unified Communications Manager Administration Guide.

Procedure

Step 1 To search for the assistant for whom you want to update information, choose User Management > End User from Cisco Unified Communications Manager Administration.

Step 2 From the Find and List Users window, click the Find button. The window displays all the end users that are configured in Cisco Unified Communications Manager.

Step 3 From the Find and List Users window, choose the assistant whose information you want to update. The End User Configuration window displays.
Step 4  From the Related Links drop-down list box, choose Assistant Configuration and click Go. The Assistant Configuration window displays for the user that you chose.

Step 5  Update the information that you want changed such as device name, intercom line, or associated manager information.

Step 6  Click the Save button. The update takes effect immediately.

Note  During automatic configuration, the system automatically sets the softkey template and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings and sets auto answer with speakerphone for intercom line. If you do not want to use automatic configuration, uncheck the Automatic Configuration check box.

Note  When non-Cisco Unified Communications Manager Assistant changes such as name, user locale, or PIN, are made to a user, the user (manager or assistant) must log out of Cisco Unified Communications Manager Assistant and log in before the changes occur.

Additional Information
See the “Related Topics” section on page 12-31.

Dial Rules Configuration

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that the assistant dials. For example, a dial rule can automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

The following sections provide additional information on application dial rules:

- Application Dial Rules Configuration Design, Cisco Unified Communications Manager System Guide
- Application Dial Rules Configuration Error Checking, Cisco Unified Communications Manager System Guide

Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants

Install the assistant console application for Cisco Unified Communications Manager Assistant by accessing a URL. The administrator sends the URL, in the “Installing the Assistant Console Plug-in” section on page 12-29, to the assistant.

Note  The assistant console application installation program supports Microsoft Internet Explorer 7, and Internet Explorer 8, FireFox 3.x and Safari 4.x.
Installing the Assistant Console Plug-in

The assistant console application installation supports Internet Explorer 7, Microsoft Internet Explorer 8, FireFox 3.x and Safari 4.x. You can install the application on a PC that runs Windows XP, Windows Vista or Apple MAC OS X.

A previous 5.x or 6.x version of the assistant console application works with Cisco Unified Communications Manager 7.1, but if you decide to install the 7.1 plug-in, you must uninstall the previous 5.x or 6.x version of the assistant console application before you install the plug-in.

Previous versions of the assistant console application do not work with Windows Vista. If the PC runs Windows Vista, install the plug-in.

After you upgrade from Cisco Unified CallManager Release 4.x to Cisco Unified Communications Manager 7.1, you must install the assistant console plug-in. Before you install the plug-in, uninstall the 4.x version of the assistant console application.

To uninstall previous versions of the assistant console application (6.0(1), 4.x, or any 5.x version before 5.1(3)), choose Start > Programs > Cisco Unified CallManager Assistant > Uninstall Assistant Console.

To uninstall a 5.1(3) or 6.1(x) assistant console application, go to the Control Panel and remove it.

Tip
The assistant console application requires that JRE1.4.2_05 exist in C:\Program Files\Cisco\Cisco Unified Communications Manager.

To install the assistant console application, perform the following procedure:

Procedure

Step 1 From the PC where you want to install the assistant console application, browse to Cisco Unified Communications Manager Administration and choose Application > Plugins.

Step 2 For the Cisco Unified Communications Manager Assistant plug-in, click the Download link; save the executable to a location that you will remember.

Step 3 Locate the executable and run it.

Tip
If you install the application on a Windows Vista PC, a security window may display. Allow the installation to continue.

The installation wizard displays.

Step 4 In the Welcome window, click Next.

Step 5 Accept the license agreement and click Next.

Step 6 Choose the location where you want the application to install. After you choose the location for the installation, click Next.

Tip
By default, the application installs in C:\Program Files\Cisco\Unified Communications Manager Assistant Console.

Step 7 To install the application, click Next.
The installation begins.

**Step 8**

After the installation completes, click **Finish**.

---

**Tip**

To launch the assistant console, click the desktop icon or choose *Cisco Unified Communications Manager Assistant > Assistant Console* in the Start...Programs menu.

Before the assistant logs in to the console, give the assistant the port number and the IP address or hostname of the Cisco Unified Communications Manager server where the Cisco IP Manager Assistant service is activated. The first time that the assistant logs in to the console, the assistant must enter the information in the Cisco Unified Communications Manager Assistant Server Port and the Cisco Unified Communications Manager Assistant Server Hostname or IP Address fields.

Before the assistant logs in to the console, give the assistant the user name and password that is required to log in to the console.

The Advanced tab in the Cisco Unified Communications Manager Assistant Settings window allows you to enable trace for the assistant console.

---

**Assistant Console Dialog Options**

The assistant console displays a dialog that contains the following options:

- **Location to Install**—The path of the directory where the assistant console software gets installed. The default specifies following path:
  - `c:\Program Files\Cisco\Unified Communications Manager Assistant Console`
- **Create Desktop Shortcut**—Default specifies true. This parameter determines whether a shortcut is created on the assistant console.
- **Create StartMenu Shortcut**—Default specifies true. This parameter determines whether a shortcut is created in the Start menu (Start > Programs > Cisco Unified Communications Manager Assistant > Assistant Console).
- **Install JRE**—Default specifies true. This parameter determines whether JRE is installed along with Unified CM Assistant assistant console. If this option is turned off, you need to ensure that the following configuration is on the assistant console:
  - Install JRE 1.4.2_05 (international version) on the assistant console
  - Create an environment variable—Assistant_JRE on the assistant console, which gives the path to the JRE; for example, `c:\Program Files\Java\j2re1.4.2_05`
Manager Configuration

Managers can customize their feature preferences from the Manager Configuration window by using the following URL:

https://<Cisco Unified Communications Manager Assistant server>:8443/ma/desktop/maLogin.jsp

where

Cisco Unified Communications Manager Assistant server specifies the IP address of the server that has the Cisco IP Manager Assistant service running on it.

Note

The Manager Configuration only supports Microsoft Internet Explorer 6.0 or later.

The administrator must send this URL to the manager.

Additional Information

See the “Related Topics” section on page 12-31.

Related Topics

- Configuration Checklist for Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-2
- Introducing Cisco Unified Communications Manager Assistant, page 12-5
- System Requirements for Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-10
- Interactions and Restrictions, page 12-11
- Installing and Activating Cisco Unified Communications Manager Assistant, page 12-15
- Configuring Cisco Unified Communications Manager Assistant with Shared Line Support, page 12-15
- Providing Information to Cisco Unified Communications Manager Assistant Managers and Assistants, page 12-28
- Cisco Unified Communications Manager Assistant With Proxy Line Support, page 11-1
- Softkey Templates, Cisco Unified Communications Manager System Guide
- Understanding Directory Numbers, Cisco Unified Communications Manager System Guide
- Directory Number Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco IP Manager Assistant Service, page 12-6
- Cisco Unified IP Phone Interface, page 12-8
- Manager and Assistant Phone Configuration, page 12-19
- Nonmanager and Nonassistant Phones, page 12-21
- Configuring a Manager and Assigning an Assistant for Shared Line Mode, page 12-22
- Deleting Cisco Unified Communications Manager Assistant Information for the Manager, page 12-24
Related Topics

- Updating the Manager Cisco Unified Communications Manager Assistant Configuration, page 12-24
- Configuring Shared and Incoming Intercom Lines for the Assistant, page 12-25
- Deleting the Cisco Unified Communications Manager Assistant Information for the Assistant, page 12-27
- End User Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Associating Devices to an End User, Cisco Unified Communications Manager Administration Guide
- Intercom, page 28-1

Additional Cisco Documentation

- Cisco Unified Communications Manager Assistant User Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
Cisco Unified Communications Manager Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant, a simple automated attendant, allows callers to locate people in your organization without talking to a receptionist. You can customize the prompts that are played for the caller, but you cannot customize how the software interacts with the customer. Cisco Unified Communications Manager Auto-Attendant comes bundled with Cisco Unified Communications Manager on the Cisco Unified Communications Manager 5 agent Cisco Unified Contact Center Express bundle.

This chapter describes Cisco Unified Communications Manager Auto-Attendant that is running on Cisco Customer Response Solutions (CRS) 5.0.

---

Note

For information about supported versions of Cisco CRS with Cisco Unified Communications Manager, see the following URL: http://www.cisco.com/univercd/cc/td/doc/systems/unified/iptmtrix.htm

To access the documentation for Cisco Customer Response Solutions, see the following URL: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Use the following topics to understand, install, configure, and manage Cisco Unified Communications Manager Auto-Attendant:

- Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant, page 13-2
- Introducing Cisco Unified Communications Manager Auto-Attendant, page 13-3
- Installing the Cisco Unified Communications Manager Auto-Attendant, page 13-6
- Configuring Cisco Unified Communications Manager Auto-Attendant and the Cisco CRS Engine, page 13-6
- Managing Cisco Unified Communications Manager Auto-Attendant, page 13-6
- Related Topics, page 13-7
Cisco Unified Communications Manager Auto-Attendant, a simple automated attendant, allows callers to locate people in your organization without talking to a receptionist. You can customize the prompts that are played for the caller, but you cannot customize how the software interacts with the customer.

Cisco Unified Communications Manager Auto-Attendant comes bundled with Cisco Unified Communications Manager on the Cisco Unified Communications Manager 5 agent Cisco Unified Contact Center Express bundle.

Table 13-1 describes the procedures that you perform to configure Cisco Unified Communications Manager Auto-Attendant. For more information on Cisco Unified Communications Manager Auto-Attendant, see the “Introducing Cisco Unified Communications Manager Auto-Attendant” section on page 13-3 and the “Related Topics” section on page 13-7.

Table 13-1  Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Install and configure Cisco Unified Communications Manager. | Installing Cisco Unified Communications Manager Release 8.5(1)  
Cisco Unified Communications Manager Administration Guide  
Cisco Unified Communications Manager System Guide |
| **Step 2**          |                               |
| Configure Cisco Unified Communications Manager users. | End User Configuration Settings, Cisco Unified Communications Manager Administration Guide |
| **Step 3**          |                               |
| Configure the Cisco Customer Response Solutions (CRS) Engine. You must install and configure Cisco CRS before you can use Cisco Unified Communications Manager Auto-Attendant. The Cisco CRS Engine controls the software and its connection to the telephony system. | These procedures can be found in the following Cisco CRS documentation:  
Cisco Customer Response Solutions Administration Guide, Release 5.0(1)  
Cisco Customer Response Solutions Installation Guide |
| • Set up the cluster, if applicable. |                               |
| • Set up the server. |                               |
| • Add a Unified CM telephony call control group. |                               |
| • Provision a Cisco media termination subsystem. |                               |
| • Add a new Cisco Unified Communications Manager Auto-Attendant. |                               |
| • Configure a Unified CM telephony trigger. |                               |
Introducing Cisco Unified Communications Manager Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant (see Figure 13-1) works with Cisco Unified Communications Manager to receive calls on specific telephone extensions. The software interacts with the caller and allows the caller to search for and select the extension of the party (in your organization) that the caller is trying to reach.

This section provides an introduction to Cisco Unified Communications Manager Auto-Attendant:

- **Cisco Unified Communications Manager Auto-Attendant Overview**, page 13-4
- **Components of Cisco Unified Communications Manager Auto-Attendant**, page 13-5

### Table 13-1 Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Customize Cisco Unified Communications Manager Auto-Attendant, so its prompts are meaningful to the way that you are using the automated attendant.</td>
<td>These procedures can be found in the following Cisco CRS documentation:</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Customer Response Solutions Administration Guide, Release 5.0(1)</em></td>
</tr>
<tr>
<td>• Modify an instance of Cisco Unified Communications Manager Auto-Attendant.</td>
<td></td>
</tr>
<tr>
<td>• Configure the Cisco Unified Communications Manager Auto-Attendant prompts.</td>
<td></td>
</tr>
<tr>
<td>- Recording the welcome prompt</td>
<td></td>
</tr>
<tr>
<td>- Configuring the welcome prompt</td>
<td></td>
</tr>
<tr>
<td>- Uploading a spoken name</td>
<td></td>
</tr>
</tbody>
</table>
Introducing Cisco Unified Communications Manager Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant provides the following functions:

- Answers a call
- Plays a user-configurable welcome prompt
- Plays a main menu prompt that asks the caller to perform one of three actions:
  - Press 0 for the operator.
  - Press 1 to enter an extension number.
  - Press 2 to spell by name.
- If the caller chooses to spell by name (by pressing 2), the system compares the letters that are entered with the names that are configured to the available extensions.
  - If a match exists, the system announces a transfer to the matched user and waits for up to 2 seconds for the caller to press any DTMF key to stop the transfer. If the caller does not stop the transfer, the system performs an explicit confirmation: it prompts the user for confirmation of the name and transfers the call to the primary extension of that user.
  - If more than one match occurs, the system prompts the caller to choose the correct extension.
  - If too many matches occur, the system prompts the caller to enter more characters.
- When the caller has specified the destination, the system transfers the call.
  - If the line is busy or not in service, the system informs the caller accordingly and replays the main menu prompt.
Components of Cisco Unified Communications Manager Auto-Attendant

The Cisco Customer Response Solutions (CRS) Platform provides the components that are required to run Cisco Unified Communications Manager Auto-Attendant. The platform provides a multimedia (voice/data/web) IP-enabled customer care application environment.

Note

Cisco CRS gets marketed under the names Cisco Unified Contact Center Express and Cisco Unified IP IVR, which are products on the Cisco CRS platform.

Cisco Unified Communications Manager Auto-Attendant uses three main components of the Cisco CRS Platform:

- **Gateway**—Connects the unified communications network to the Public Switched Telephone Network (PSTN) and to other private telephone systems such as Public Branch Exchange (PBX). You must purchase gateways separately.
- **Cisco Unified Communications Manager Server**—Provides the features that are required to implement IP phones, manage gateways, provides failover and redundancy service for the telephony system, and directs voice over IP traffic to the Cisco CRS system. You must purchase Cisco Unified Communications Manager separately.
- **Cisco CRS Server**—Contains the Cisco CRS Engine that runs Cisco Unified Communications Manager Auto-Attendant. The Cisco Unified Communications Manager Auto-Attendant package includes the Cisco CRS Server and Engine.

For more information about the Cisco CRS Platform, see the following URL.


System Requirements for Cisco Unified Communications Manager Auto-Attendant

Cisco Unified Communications Manager Auto-Attendant requires the following software components to operate:

- Cisco Unified Communications Manager
- Cisco CRS Release 5.0

Cisco Unified Communications Manager Auto-Attendant runs on the Cisco Media Convergence Server (Cisco MCS) platform or on a Cisco-certified server.

See the following Cisco documentation:

Installing the Cisco Unified Communications Manager Auto-Attendant

No installation is required. Auto-Attendant comes standard with the five-seat bundle. See the Cisco Customer Response Solutions Administration Guide, Release 5.0(1) and the Cisco Customer Response Solutions Installation Guide for more information.

Additional Information
See the “Related Topics” section on page 13-7

Configuring Cisco Unified Communications Manager Auto-Attendant and the Cisco CRS Engine

To configure the Cisco Unified Communications Manager Auto-Attendant, review the “Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant” section on page 13-2.

Managing Cisco Unified Communications Manager Auto-Attendant

Use Cisco CRS Administration to manage Cisco Unified Communications Manager Auto-Attendant. Use the online help to learn how to use the interface and perform these tasks. Table 13-2 describes the management tasks.

Table 13-2  Managing Cisco Unified Communications Manager Auto-Attendant

<table>
<thead>
<tr>
<th>Task</th>
<th>Purpose</th>
<th>Commands (from the Cisco CRS Administration main window)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and stop the Cisco CRS Engine</td>
<td>Make sure that the engine is running for your automated attendant to work. You can stop and restart the engine to help resolve or troubleshoot problems.</td>
<td>Choose System &gt; Control Center and click the Cisco CRS Engine in the menu on the left. In the list that appears, find “CRS Engine”. In the Status column, if a triangular button points to the right, you know that the engine is running. If a square shows in this column, you know that the engine is not running. To restart the engine, click the radio button next to “CRS Engine” and click Restart. If the engine is running and you want to stop it, click the radio button next to “CRS Engine” and click Stop.</td>
</tr>
<tr>
<td>Change the Cisco CRS Engine configuration</td>
<td>Modify the engine configuration to resolve problems.</td>
<td>Choose System &gt; System Parameters.</td>
</tr>
</tbody>
</table>
### Table 13-2 Managing Cisco Unified Communications Manager Auto-Attendant (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Purpose</th>
<th>Commands (from the Cisco CRS Administration main window)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up trace files</td>
<td>Set up trace files to collect troubleshooting information.</td>
<td>Choose System &gt; Tracing; then, click Trace File Configuration. See the online help for detailed information.</td>
</tr>
<tr>
<td>View trace files</td>
<td>View trace files to see the results of your tracing.</td>
<td>Choose System &gt; Control Center; then, click server name. Click the Server Traces link. Choose the trace file that you created.</td>
</tr>
<tr>
<td>Monitor performance in real time</td>
<td>You can monitor the performance of the system while it is running if you install the real-time reporting monitor.</td>
<td>Choose Tools &gt; Real-Time Reporting. See the online help for information on using Real Time Reporting.</td>
</tr>
</tbody>
</table>

**Additional Information**

See the “Related Topics” section on page 13-7

### Related Topics

- Configuration Checklist for Cisco Unified Communications Manager Auto-Attendant, page 13-2
- Introducing Cisco Unified Communications Manager Auto-Attendant, page 13-3
- Cisco Unified Communications Manager Auto-Attendant Overview, page 13-4
- Components of Cisco Unified Communications Manager Auto-Attendant, page 13-5
- System Requirements for Cisco Unified Communications Manager Auto-Attendant, page 13-5
- Installing the Cisco Unified Communications Manager Auto-Attendant, page 13-6
- Configuring Cisco Unified Communications Manager Auto-Attendant and the Cisco CRS Engine, page 13-6
- Managing Cisco Unified Communications Manager Auto-Attendant, page 13-6
Cisco Unified Mobility extends the rich call control capabilities of Cisco Unified Communications Manager from the primary workplace desk phone of a mobile worker to any location or device of their choosing.

For example, Cisco Unified Mobility associates a user mobile phone number with the user business IP phone number. Cisco Unified Mobility then directs incoming calls to ring on a user mobile phone as well as the business phone, thus providing a single number for callers to reach the user. Calls that go unanswered on all the designated devices get redirected to the enterprise voice mailbox of the user (not to the mobile voice mailbox).

Administrators can configure Cisco Unified Mobility, formerly known as Cisco Unified MobilityManager, by using the Cisco Unified Communications Manager Administration windows to configure the setup for end users. End users can use Cisco Unified CM User Options windows to configure their own personal settings.

Cisco Unified Mobility comprises a number of features that this chapter discusses. The chapter provides an overview of the configuration procedures that administrators follow.

See the user guide for a particular Cisco Unified IP Phone model for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified CM User Options windows.

For explanations and configuration of features that are related to Cisco Unified Mobility and that require additional configuration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator, see the “Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration” chapter. The chapter also points to other documentation that explains configuration of Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator.

This chapter includes information on the following topics:

- Configuration Checklist for Cisco Unified Mobility, page 14-2
- Introducing Cisco Unified Mobility, page 14-4
  - Definitions, page 14-5
  - List of Cisco Unified Mobility Features, page 14-6
  - Other Benefits of Cisco Unified Mobility Features, page 14-7
  - Mobile Connect, page 14-8
  - Desktop Call Pickup, page 14-10
  - Send Call to Mobile Phone, page 14-10
Cisco Unified Mobility gives users the ability to redirect incoming IP calls from the Cisco Unified Communications Manager to up to ten different designated client devices such as mobile phones. For more information on Cisco Unified Mobility features, see the “List of Cisco Unified Mobility Features” section on page 14-6.

Table 14-1 summarizes the procedures for configuring Cisco Unified Mobility. For detailed instructions, see the chapters and sections that the table references. In addition, see the “Related Topics” section on page 14-62.
### Table 14-1  Cisco Unified Mobility Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Activate the Cisco Unified Mobile Voice Access Service in Cisco Unified Serviceability. You must activate this service on the first node in the cluster.</td>
<td>For information on activating services, See the <em>Cisco Unified Serviceability Administration Guide</em>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Configure user accounts.</td>
<td>End User Configuration, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For information on how licensing works with Mobile Connect, See “Licenses for Cisco Unified Mobility”.</td>
</tr>
<tr>
<td>Checking the Enable Mobility check box triggers User Connect License (UCL) to provide licensing for Mobile Connect.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Create access lists for Mobile Connect by assigning each list to the Mobile Connect user and specifying whether the list is an allowed or blocked list.</td>
<td>Access List Configuration, page 14-36.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Create remote destination profiles and assign each user to a profile.</td>
<td>Remote Destination Profile Configuration, page 14-39.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>Associate desktop directory numbers (DNs) for the user.</td>
<td>Associating a Directory Number with a Remote Destination Profile, page 14-43.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>Add remote destinations by selecting the previously-defined profile as part of the configuration.</td>
<td>Remote Destination Configuration, page 14-43.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>In the Service Parameters Configuration window:</td>
<td>Service Parameter Configuration, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td>• Choose True for Enable Mobile Voice Access and enter the Mobile Voice Access Number, which is the DID number that end users use to reach Mobile Voice Access.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To make Mobile Voice Access calls, you must configure these service parameters and check the Enable Mobile Voice Access check box in the End User Configuration window.</td>
</tr>
<tr>
<td>• Choose True for Enable Enterprise Feature Access to enable access to hold, resume, transfer, and conference features from remote destinations.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
</tbody>
</table>
Introducing Cisco Unified Mobility

Administrators configure the basic setup of Cisco Unified Mobility for end users by using the Cisco Unified Communications Manager Administration windows.

This section discusses the following topics:

- Definitions, page 14-5
- List of Cisco Unified Mobility Features, page 14-6
- Other Benefits of Cisco Unified Mobility Features, page 14-7
- Mobile Connect, page 14-8
- Desktop Call Pickup, page 14-10
- Send Call to Mobile Phone, page 14-10
- Mobile Voice Access, page 14-11
- Midcall Enterprise Feature Access Support Using DTMF, page 14-12
- Two-Stage Dialing, page 14-12
- Time-of-Day Access, page 14-12
- Directed Call Park via DTMF, page 14-15
- SIP URI Dialing, page 14-16
- Intelligent Session Control, page 14-17
- Session Handoff, page 14-19
- Use Case Scenarios for Cisco Unified Mobility Features, page 14-21

### Table 14-1  Cisco Unified Mobility Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td>As an alternative, configure Enterprise Feature Access Two-Stage Dialing (also known as Enterprise Feature Access) by configuring a service parameter and the enterprise feature access DID directory number.</td>
</tr>
<tr>
<td>Note</td>
<td>Enterprise Feature Access provides the same functionality as Mobile Voice Access but does not support the IVR component. Also, Enterprise Feature Access does not require configuration of the H.323 gateway nor VXML.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Configure mobility settings for dual-mode phone handoff.</td>
</tr>
<tr>
<td></td>
<td>Handoff Mobility Configuration Settings, page 14-57.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Configure a Mobility softkey for the phone user that uses Mobile Connect.</td>
</tr>
<tr>
<td></td>
<td>Mobility Softkey Configuration, page 14-61</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Configure time-of-day access for users. Use the fields in the When Mobile Connect is Enabled pane of the Remote Destination Configuration window to do so.</td>
</tr>
<tr>
<td></td>
<td>Remote Destination Configuration, page 14-43.</td>
</tr>
</tbody>
</table>
Additional Information
See the “Related Topics” section on page 14-62.

Definitions

Table 14-2 provides definitions of terms that are related to Cisco Unified Mobility.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access List</td>
<td>List that determines the phone numbers that the system can pass or block from being passed to remote destinations.</td>
</tr>
<tr>
<td>Session Handoff</td>
<td>Transfer of session/conversations such as voice, video, and meetings between various Unified Communications clients that associate with a single user.</td>
</tr>
<tr>
<td>Types of Session Handoff</td>
<td>Two-touch Session Handoff—In this type, no Unified Communications client proximity detection logic gets used; all devices under the same user ring and first one to accept gets the call.</td>
</tr>
<tr>
<td>Enterprise Feature Access</td>
<td>Feature that provides the ability for users to access midcall features (Hold, Resume, Transfer, Conference, Directed Call Park), two-stage dialing, and Mobile Connect activate and deactivate from a remote destination. With this method, the user does not get prompted for keypad entries and must be aware of the required key sequence.</td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Feature that allows users to answer incoming calls on the desk phone or at a remote destination and to pick up in-progress calls on the desk phone or at a remote destination without losing the connection.</td>
</tr>
<tr>
<td>Mobile Voice Access</td>
<td>Interactive voice response (IVR) system that is used to initiate two-stage dialed calls through the enterprise and to activate or deactivate Mobile Connect capabilities.</td>
</tr>
<tr>
<td>Remote Destination Profiles</td>
<td>Set of parameters that apply to all remote destinations for the user.</td>
</tr>
<tr>
<td>Time-of-Day Access</td>
<td>Feature that associates ring schedules to access lists and determines whether a call will be extended to a remote destination during the time of day when such a call is received.</td>
</tr>
<tr>
<td>Toast</td>
<td>A pop-up indication that expects user input.</td>
</tr>
</tbody>
</table>
Additional Information

See the “Related Topics” section on page 14-62.

List of Cisco Unified Mobility Features

This section provides a list of Cisco Unified Mobility features that administrators configure by using Cisco Unified Communications Manager Administration.

The following features, which were originally part of Cisco Unified Mobility Manager, now reside in Cisco Unified Communications Manager:

• Mobile Connect—This feature enables users to manage business calls by using a single phone number to pick up in-progress calls on the desk phone and the mobile phone. See the “Mobile Connect” section on page 14-8 for a detailed discussion.

• Desktop Call Pickup—Users can switch between desk phone and mobile phone during an active call without losing the connection. Based on the needs of the moment, they can take advantage of the reliability of the wired office phone or the mobility of the mobile phone. See the “Desktop Call Pickup” section on page 14-10 for a detailed discussion.

• Send Call to Mobile Phone(s)—Users access this feature on the IP phone via the Mobility softkey. The feature triggers a remote destination pickup, which allows the user to move an active mobility call from the user desk phone to a configured remote destination phone. See the “Send Call to Mobile Phone” section on page 14-10 for a detailed discussion.

• Mobile Voice Access—This feature extends Mobile Connect capabilities by providing an interactive voice response (IVR) system to initiate two-stage dialed calls through the enterprise and activate or deactivate Mobile Connect capabilities. See the “Mobile Voice Access” section on page 14-11 for a detailed discussion.

• Access List—Users can restrict the set of callers that cause a designated remote destination to ring on an incoming call (allowed access list) or for which the remote destinations do not ring on an incoming call (blocked access list). Each remote destination represents a mobile or other phone that can be configured to accept transfers from the desk phone for the user.

Cisco Unified Communications Manager supports the following Cisco Unified Mobility features:

• Midcall Enterprise Feature Access Support Using DTMF—You can configure DTMF feature codes as service parameters: enterprise hold (default equals *81), enterprise exclusive hold (default equals *82), resume (default equals *83), transfer (default equals *84), and conference (default equals *85). See the “Midcall Enterprise Feature Access Support Using DTMF” section on page 14-12 for a detailed discussion.

Note

*81 specifies enterprise hold. When invoked, enterprise hold allows the user to resume the call on the desk phone. *82 specifies enterprise exclusive hold. When invoked, enterprise exclusive hold does not provide the ability to resume the call on the desk phone. If a mobility call that is on enterprise hold disconnects in this state, the user can resume the call on the desk phone. Alternatively, if a mobility call that is on enterprise exclusive hold disconnects in this state, the user cannot resume the call on the desk phone.

• Two-stage Dialing—Be aware that enterprise features are available with two-stage dialing for smartphones. Two-stage dialing allows smartphones to make outgoing calls through Cisco Unified Communications Manager if the smartphone is in business mode. The smartphone dials the Enterprise Feature Access number for Cisco Unified Communications Manager and then dials the destination number. See the “Two-Stage Dialing” section on page 14-12 for a detailed discussion.
- Dual-mode Phone Support—Cisco Unified Mobility supports dual-mode phones.
- Manual Handoff of Calls on a Dual-mode Phone—Dual-mode devices offer an option to manually hand off calls from the PSTN to WLAN and vice versa.
- Time-of-Day Access—When the Mobile Connect feature is enabled, calls get extended to remote destinations if the associated DN is called based on time-of-day-access-based configuration. See the “Time-of-Day Access” section on page 14-12 for a detailed discussion.
- Directed Call Park via DTMF—This feature allows a mobile phone user to park a call by transferring the parked party to a park code, so the call can be retrieved later. The feature combines the standard Cisco Unified Communications Manager Directed Call Park feature with the DTMF feature. Support of the Directed Call Park via DTMF feature leverages the Midcall Enterprise Transfer feature. See the “Directed Call Park via DTMF” section on page 14-15 for a detailed discussion.
- SIP URI Dialing—This feature supports SIP URI as an additional type of remote destination for Cisco Unified Mobility. See the “SIP URI Dialing” section on page 14-16 for a detailed discussion.
- Intelligent Session Control—This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only, the call was not anchored to the user desk phone, and the mobile user could not invoke any mobility features.) During such calls, the user can invoke mobility features such as midcall features and Session Handoff from the user mobile phone. See the “Intelligent Session Control” section on page 14-17 for a detailed discussion.
- Session Handoff—This feature leverages the existing Cisco Unified Communications Manager experience by allowing the user to move voice, video, and meeting sessions and conversations between different Unified Communications clients, such as Cisco Unified Personal Communicator (running on a PC in Softphone as well as CTI control mode), Cisco Unified Mobile Communicator (running on a mobile phone), and Cisco Unified IP Phone Series 9900 and legacy phones that are running SIP.

The conversation can be moved from mobile phone to any other Unified Communications client. All devices that the user owns and that share the same line ring or show a toast, and the call gets answered by whichever device picks it up first. Upon answer, all the other shared-line devices enter Remote in Use mode. See the “Session Handoff” section on page 14-19 for a detailed discussion.

Note that the only client that can actually hand off a session (because it is the only client that has an anchored DTMF path back to Cisco Unified Communications Manager) is Cisco Unified Mobile Communicator. Neither Cisco Unified Personal Communicator nor 9900 series Cisco Unified IP Phones can initiate a session handoff. These devices can, however, handle an incoming session handoff.

Additional Information

See the “Related Topics” section on page 14-62.

**Other Benefits of Cisco Unified Mobility Features**

Cisco Unified Mobility allows flexible management of enterprise and mobile phone communications and provides these additional features and benefits:

- Simultaneous desktop ringing—Incoming calls ring simultaneously on the IP phone extension and the designated mobile handset. When the user answers one line, the unanswered line automatically stops ringing. Users can choose the preferred device each time that a call comes in.
Introducing Cisco Unified Mobility

- Single enterprise voice mailbox—The enterprise voice mailbox can serve as single, consolidated voice mailbox for all business, including calls to the desktop or configured remote devices. Incoming callers have a predictable means of contacting employees, and users can check multiple voice-messaging systems in less time.

- System remote access—A mobile phone for the user can initiate calls as if it were a local IP PBX extension. User-initiated calls can take advantage of local voice gateways and WAN trunking, and the enterprise can track employee call initiation.

- Caller ID—The system preserves and displays Caller ID on all calls. Users can take advantage of Mobile Connect with no loss of expected IP phone features.

- Remote on/off control—User can turn Mobile Connect feature. See “Methods for Enabling and Disabling Mobile Connect” section on page 14-8 for details.

- Call tracing—The system logs detailed Mobile Connect calls and provides information to help the enterprise optimize trunk usage and debug connection problems.

- Security and privacy for Mobile Connect calls—During an active Mobile Connect call, the associated desktop IP phone remains secured. The system eliminates access to the call from the desktop as soon as the mobile connection becomes active, which precludes the possibility of an unauthorized person listening in on the call that is bridged to the mobile phone.

Additional Information
See the “Related Topics” section on page 14-62.

Mobile Connect

Mobile Connect allows users to answer incoming calls on the desk phone or mobile phone, and to pick up in-progress calls on the desk phone or mobile phone without losing the connection.

Note
You can use any mobile phone, including Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) phones, for Mobile Connect and Mobile Voice Access. In some cases, however, you may need to modify timer settings in Cisco Unified Communications Manager to ensure compatibility. See the “Remote Destination Configuration” section on page 14-43.

Methods for Enabling and Disabling Mobile Connect

The following methods are available for enabling and disabling the Mobile Connect feature. This list provides the methods that are available to the administrator and to end users.

- Cisco Unified Communications Manager Administration windows. Menu path specifies Device > Phone, then configure the Mobility Identity of the Cisco Unified Mobile Communicator by checking the Enable Mobile Connect check box (to enable Mobile Connect) or by unchecking this check box (to disable Mobile Connect).

- Cisco Unified CM User Options windows: URL specifies http://<Unified CM IP address>/ccmuser. Within the application, specify the User Options > Mobility Settings > Remote Destinations > Enable Mobile Connect menu path.

- Desk phone by using the Mobility softkey. To configure, use these menu options:
  - Device > Phone, and specify the Mobility softkey template in the Softkey Template field.
  - Device > Phone, and assign the same mobility user ID on the remote destination profile as the desk phone owner user ID.
Mobile phone by using Mobile Voice Access (uses IVR prompts; 2 to enable or 3 to disable)

Mobile phone by using Enterprise Feature Access (after PIN entry, 2 to enable or 3 to disable). The sequence specifies <PIN>#2# or <PIN>#3#.

Cisco Unified Mobile Communicator client: The client offers the mobile user the option to change the user Mobile Connect status. See “Enable/Disable Mobile Connect From Mobile Phone” section on page 16-6 for details.

**Mobile Connect Status**

If at least one configured remote destination for a user is enabled for Mobile Connect, the user desk phone displays Mobile Connect as Enabled.

**RDNIS/Diversion Header**

The RDNIS/diversion header for Mobile Connect enhances this Cisco Unified Mobility feature to include the RDNIS or diversion header information on the forked call to the mobile device. Service providers and customers use the RDNIS for correct billing of end users who make Cisco Unified Mobility Mobile Connect calls.

For Mobile Connect calls, the Service Providers use the RDNIS/diversion header to authorize and allow calls to originate from the enterprise, even if the caller ID does not belong to the enterprise Direct Inward Dial (DID) range.

**Example RDNIS/Diversion Header Use Case**

Consider a user that has the following setup:

- Desk phone number specifies 89012345.
- Enterprise number specifies 4089012345.
- Remote destination number specifies 4088810001.

User gets a call on desk phone number (89012345) that causes the remote destination (4088810001) to ring as well.

If the user gets a call from a nonenterprise number (5101234567) on the enterprise number (4089012345), the user desk phone (89012345) rings, and the call gets extended to the remote destination (4088810001) as well.

Prior to the implementation of the RDNIS/diversion header capability, the fields populated as follows:

- Calling Party Number (From header in case of SIP): 5101234567
- Called Party Number (To header in case of SIP): 4088810001

After implementation of the RDNIS/diversion header capability, the Calling Party Number and Called Party Number fields populate as before, but the following additional field gets populated as specified:

- Redirect Party Number (Diversion Header in case of SIP): 4089012345

Thus, the RDNIS/diversion header specifies the enterprise number that is associated with the remote destination.

**Configuration of RDNIS/Diversion Header in Cisco Unified Communications Manager Administration**

To enable the RDNIS/diversion header capability for Mobile Connect calls, ensure the following configuration takes place in Cisco Unified Communications Manager Administration:

All gateways and trunks must specify that the Redirecting Number IE Delivery — Outbound check box gets checked.
In Cisco Unified Communications Manager Administration, you can find this check box by following the following menu paths:

- For H.323 and MGCP gateways, execute Device > Gateway and find the gateway that you need to configure. In the Call Routing Information - Outbound calls pane, ensure that the Redirecting Number IE Delivery - Outbound check box gets checked. For T1/E1 gateways, check the Redirecting Number IE Delivery - Outbound check box in the PRI Protocol Type Information pane.

- For SIP trunks, execute Device > Trunk and find the SIP trunk that you need to configure. In the Outbound Calls pane, ensure that the Redirecting Diversion Header Delivery - Outbound check box gets checked.

Use Case Scenarios for Mobile Connect

See the “Use Case Scenarios for Mobile Connect” section on page 14-21 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Desktop Call Pickup

User can perform desktop call pickup on in-progress mobility calls either by hanging up the call on the mobile phone or by putting the mobility call on hold with the midcall hold feature. When hanging up or ending the call at the mobile phone, the user can then resume the call on the desk phone within 10 seconds (default). When the remote destination hangs up, Cisco Unified Communications Manager puts the associated desk phone in Hold state, which allows the user to resume the call by pressing the Resume softkey. The Maximum Wait Time for Desk Pickup setting on the End User Configuration window determines the amount of time the call remains on hold after the hang-up at the remote destination. The default specifies 10000 milliseconds (10 seconds).

Alternatively, the user can also perform desktop call pickup by placing the call on the mobile phone on enterprise hold with the midcall hold feature (*81) and then resuming the call on the desk phone. When Cisco Unified Communications Manager receives the *81, Cisco Unified Communications Manager places the associated desk phone in a Hold state so the user can resume the call. Note that with this method, the Maximum Wait Time for Desk Pickup timer does not apply to the hold state and the call gets held indefinitely until the user resumes the call.

Send Call to Mobile Phone

User can perform remote destination pickup on in-progress mobility calls by using the Send Call to Mobile Phone feature. To do so, the user presses the Mobility softkey on the desk phone and selects Send Call to Mobile Phone, which generates calls to all of the remote destinations that are configured for the user. The user can then answer this call at the desired remote destination and continue the call.

When a desk phone invokes the Send Call to Mobile Phone feature and the remote destination specifies a dual-mode smartphone, the following behavior results:

- If the dual-mode smartphone is registered to Wi-Fi, the call gets sent to the device Wi-Fi side.
• If the dual-mode smartphone is not registered to Wi-Fi, the call gets sent to the device cellular side.

Additional Information
See the “Related Topics” section on page 14-62.

Mobile Voice Access

Mobile Voice Access extends Mobile Connect capabilities by allowing users to originate a call from a remote destination such as a mobile phone as if dialing from the desk phone. A remote destination represents a phone that is designated as available for Mobile Connect answer and pickup. The user dials Mobile Voice Access from the remote destination. The system prompts the user for the PIN that is assigned to the user in Cisco Unified Communications Manager. After being authenticated, the user can make a call by using the same dialing methods that would be available if the user originated the call from the enterprise desk phone.

When Mobile Voice Access is called, the system prompts the user for the originating phone number in addition to the PIN if any of the following statements is true:

• The number from which the user is calling does not represent one of the remote destinations for the user.
• The user or the carrier for the user blocks the number (shown as “Unknown Number”).
• The number does not get accurately matched in the Cisco Unified Communications Manager database; for example, if the number is 510-666-9999, but it is listed as 666-9999 in the database, or the number is 408-999-6666, but it is entered as 1-408-999-6666 in the database.
• Mobile Voice Access gets configured in hairpin mode. (When Mobile Voice Access that is configured in hairpin mode is used, users who are calling the system do not get identified automatically by their caller ID. Instead, users must manually enter their remote destination number prior to entering their PIN number.)

If the user incorrectly enters any requested information (such as mobile phone number or PIN) three times in a row, the Mobile Voice Access call can disconnect, and the system will lock out the user for a period of time. (The credential information for the user controls the allowed number of login attempts.)

Note
Mobile Voice Access uses the first locale that displays in the Selected Locales pane in the Mobile Voice Access window in Cisco Unified Communications Manager Administration (Media Resources > Mobile Voice Access) when the IVR is used. For example, if English United States displays first in the Selected Locales pane, the Cisco Unified Mobility user receives English when the IVR is used during a call.

See the “Use Case Scenarios for Mobile Voice Access” section on page 14-22 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Additional Information
See the “Related Topics” section on page 14-62.
Midcall Enterprise Feature Access Support Using DTMF

Users can leverage enterprise media resources and capabilities by invoking midcall features. DTMF digits that are relayed from the remote destination in-band in the audio path and then relayed out-of-band from the enterprise gateway to Cisco Unified Communications Manager invoke midcall features. When Cisco Unified Communications Manager receives the DTMF digits, appropriate midcall features get facilitated based on the DTMF digit sequence. Such features include adding or remove call legs for transferred or conferenced calls, as well as invoking media resources like music on hold for held calls and conference bridges as required.

The feature access codes that are configured within Cisco Unified Communications Manager under Service Parameters determine the midcall feature DTMF code sequences.

Additional Information
See the “Related Topics” section on page 14-62.

Two-Stage Dialing

The user can originate calls from the remote destination phone through the enterprise by leveraging the enterprise telephony infrastructure. Two-stage dialing provides the following benefits:

- The ability to make calls through the enterprise, which leads to centralized billing and call detail records. This ability provides the potential for cost savings by ensuring that international calls get billed to the enterprise rather than to the mobile or cellular plan. However, this capability does not eliminate normal per-minute local/long-distance charges at the mobile phone.
- The ability to mask the mobile phone number from the far-end or dialed phone. Instead of sending the mobile number to the called party, the user enterprise number gets sent to the called party during a two-stage dialed call. This method effectively masks the user mobile number and ensures that returned calls get anchored in the enterprise.

Additional Information
See the “Related Topics” section on page 14-62.

Time-of-Day Access

An access list determines whether a call should be extended to a remote destination that is enabled for the Mobile Connect feature. With the addition of time-based control, the Time-of-Day Access feature adds time as another determination factor. The feature allows administrators and users to determine whether a call should reach a remote destination based on the time of day when the call is received.

For calls to remote destinations, the Time-of-Day Access feature adds a ring schedule and associates the ring schedule with an access list to determine the time-of-day access settings for a remote destination.

The provisioning process includes provisioning the following entities:
- Access lists
- Remote destinations (configuring a ring schedule and associating the ring schedule with an access list for a remote destination)
As an extension to the existing access list feature, ensure the Time-of-Day Access feature is accessible to end users of Cisco Unified Communications Manager. Therefore, you can provision the feature through use of both Cisco Unified Communications Manager Administration (by administrators) and Cisco Unified CM User Options (by end users).

**Further Topics**

This section includes the following topics:

- Time-of-Day Access Configuration, page 14-13
- Important Notes for Time-of-Day Access, page 14-14

The “Use Case Scenarios for Time-of-Day Access” section on page 14-22 provides use case scenarios for the time-of-day access feature with Cisco Unified Mobility, including migration considerations when migrating from a release of Cisco Unified Communications Manager prior to Release 7.0(x) or later.

**Additional Information**

See the “Related Topics” section on page 14-62.

### Time-of-Day Access Configuration

Table 14-3 summarizes the procedures for configuring the Time-of-Day Access feature for Cisco Unified Mobility. For detailed instructions, see the chapters and sections that the table references.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>End User Configuration, Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>In Cisco Unified Communications Manager Administration,</td>
<td>For information on how licensing works with Mobile Connect, see the “Licenses for Cisco Unified Mobility” section in the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>configure an end user for whom you will enable the</td>
<td></td>
</tr>
<tr>
<td>Time-of-Day Access feature.</td>
<td></td>
</tr>
<tr>
<td>Use the User Management &gt; End User menu option.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>Make sure that you check the Enable Mobility check box</td>
<td></td>
</tr>
<tr>
<td>in the End User Configuration window.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>Checking the Enable Mobility check box triggers licensing</td>
<td></td>
</tr>
<tr>
<td>to consume device license units (DLUs) for Mobile Connect.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Access List Configuration, page 14-36</strong></td>
</tr>
<tr>
<td>For a particular user, configure access lists to use for</td>
<td></td>
</tr>
<tr>
<td>Time-of-Day Access by assigning each list to the user.</td>
<td></td>
</tr>
<tr>
<td>Create separate access lists for callers that are allowed</td>
<td></td>
</tr>
<tr>
<td>and callers that are blocked.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>An access list must have an owner. No system access list</td>
<td></td>
</tr>
<tr>
<td>exists.</td>
<td></td>
</tr>
<tr>
<td>Use the Call Routing &gt; Class of Control &gt; Access List</td>
<td></td>
</tr>
<tr>
<td>menu option.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Remote Destination Profile Configuration, page 14-39.</strong></td>
</tr>
<tr>
<td>Create remote destination profiles and assign each user</td>
<td></td>
</tr>
<tr>
<td>to a profile.</td>
<td></td>
</tr>
</tbody>
</table>
Introducing Cisco Unified Mobility

Additional Information

See the “Related Topics” section on page 14-62.

Important Notes for Time-of-Day Access

The following important notes apply to time-of-day access configuration:

- A ring schedule associates with the time zone of a remote destination, not with the time zone of the Cisco Unified Communications Manager server. Use the Time Zone field in the Remote Destination Configuration window to specify the time zone of the remote destination.

- If a remote destination has no time-of-day access configuration, all calls get extended to the remote destination. By default, the All the time ring schedule radio button and the Always ring this destination radio button are checked, so that all calls get extended to the remote destination.

- Cisco recommends that you always configure an access list with members; avoid creating an empty access list that contains no members. If an empty access list is chosen in the Ring this destination only if the caller is in drop-down list box, all calls get blocked (instead of allowed). If an empty access list is chosen in the Do not ring this destination if the caller is in drop-down list box, all calls are allowed during the specified ring schedule. Either use of an empty access list could cause unnecessary confusion for end users.
See the “Use Case Scenarios for Time-of-Day Access” section on page 14-22 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

See the user guide for the applicable Cisco Unified IP Phone model for details of the settings that end users can configure to customize their time-of-day access settings by using the Cisco Unified CM User Options windows.

**Additional Information**

See the “Related Topics” section on page 14-62.

---

**Directed Call Park via DTMF**

A user can park an existing call by using DTMF digits. Using Directed Call Park from the mobile phone, a user parks a call and inputs a unique mobility user park code. The user can subsequently retrieve the call with the code or have someone else retrieve the call with the code. This feature proves useful for certain vertical markets that require different departments or users to pick up calls.

When a user is in the enterprise and picks up a call on their mobile phone, they may want to pick the call up on a Cisco Unified IP Phone in a conference room or desk where the DN is not visible. The user can park the call and pick up the parked call with only their code.

When the mobile phone user is on an active call, the user can park the call by transferring the parked party to the park code that the system administrator configures and assigns to the user. The dialing sequence resembles the DTMF transfer sequence, except that a preconfigured parking code replaces the transfer number.

**Example of Directed Call Park via DTMF—Parking the Call**

In the following example, *82 specifies enterprise exclusive hold, *84 specifies transfer, the pin specifies 12345, and the call park code specifies 3215. The following actions take place from the mobile phone:

1. Dial *82 (to put the call on enterprise exclusive hold).
2. If necessary, put the mobile phone call on Hold, depending on the mobile phone model.
3. Make a new call to the Enterprise Feature Access DID.

This same DID gets used for the Enterprise Feature Access two-stage dialing feature. Configure this DID with the **Call Routing > Mobility > Enterprise Feature Access Configuration** menu option.

4. After the call connects, dial the following field-and-digit sequence: `<PIN>#$84#$Park Code>#$84#`

   For example, if the PIN specifies 12345 and park code specifies 3215, the digit sequence would be `12345#$84#3215#$84#`

Cisco Unified Communications Manager puts the parked party on hold.

---

The caller ID of the mobile phone must get passed to the enterprise and must match a configured remote destination when the user dials the Enterprise Feature Access DID to invoke this feature. If no caller ID exists or no caller ID match occurs, the user cannot invoke this feature.

After Cisco Unified Communications Manager receives the dialed park code digit, the digit analysis engine verifies whether the dialed park code digits are valid. If so, the Directed Call Park feature intercepts the park code and verifies whether the park code is available. If the dialed park code is valid
and available, the parking party receives the ringback tone, and the secondary call terminates to a Cisco Unified Communications Manager generic device that associates with the selected park code. The generic device automatically answers and place the parking party on hold with music on hold (MOH) or tone on hold. The last *84 completes the transfer of the parked party to the Cisco Unified Communications Manager generic device that associates with the selected park code. After the transfer completes, the parked party receives the MOH or tone on hold, and the parked party gets parked on this selected park code and waits for retrieval.

If another user is already using the user-specified park code, Directed Call Park feature logic in Cisco Unified Communications Manager rejects that selected park code. The user gets to select another park code.

If the user-specified park code is not valid, Cisco Unified Communications Manager plays reorder tone to the parking party.

For the Directed Call Park feature, be aware that the park code and code range are configurable across a cluster. Every Cisco Unified Communications Manager server in the cluster shares the park code and code range.

**Example of Directed Call Park via DTMF—Retrieving the Parked Call**

When a user attempts to retrieve the parked call, the user can go off hook on another mobile phone, and the user must use two-stage dialing to dial a digit string that contains the Directed Call Park retrieval prefix digits (for example, 22) plus the park code/code range (for example, 3215). The following sequence of events takes place:

1. Dial Enterprise Feature DID on mobile phone.
2. Upon connection, dial the following field-and-digit sequence to retrieve the parked call:

   \[
   \text{<PIN>}#1#\text{<Retrieval Prefix>}\text{<Park Number>}#
   \]

   In our example, the full sequence specifies 12345#1#223215# to retrieve the parked call.

Just like the existing Call Park feature, if the call does not get retrieved on time, the parked call reverts back to the phone number that is associated with the parking party by default.

If a shared line is configured for the phone line of the parking party, all phones that are associated with the shared line will ring. In addition, the dPark feature allows the administrator to configure a call park reversion number in the Directed Call Park Configuration window, so if the call park reversion number is configured, the non-retrieved call reverts to this number, instead of to the parking party number.

See the “Use Case Scenarios for Directed Call Park via DTMF” section on page 14-23 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

**Additional Information**

See the “Related Topics” section on page 14-62.

---

**SIP URI Dialing**

This feature supports Session Initiation Protocol (SIP) Universal Resource Identifier (URI) as an additional type of remote destination for Cisco Unified Mobility. When the DN is called, Cisco Unified Communications Manager extends the call to a SIP trunk that digit analysis selects with this SIP URI in the To: header.

This feature only allows routing that is based only on the domain name, not based on the full SIP URI.
When a remote destination of this type is configured, other Cisco Unified Mobility features, such as two-stage dialing, transformation to DN number when calling into Cisco Unified Communications Manager, Interactive Voice Response (IVR) support, caller ID match, or DTMF transfer and conferencing, do not get supported.

**SIP URI Administration Details**

The SIP URI dialing feature entails a relaxation of the business rules to allow the entry of a URI in the Destination Number field of the Remote Destination Configuration window. (From the Cisco Unified Communications Manager Administration menu bar, choose the Device > Remote Destination menu option.)

An additional requirement for this feature specifies that a SIP route pattern that matches the configured URI domain must be configured for the feature to work. To configure a SIP route pattern, from the Cisco Unified Communications Manager Administration menu bar, choose the Call Routing > SIP Route Pattern menu option.

**SIP URI Example**

For a remote destination, the SIP URI `user@corporation.com` gets configured. A SIP route pattern that specifies `corporation.com` must also get configured for the SIP URI remote destination to resolve correctly.

**Additional Information**

See the “Related Topics” section on page 14-62.

**Intelligent Session Control**

This feature modifies the behavior of outgoing calls placed from the enterprise directly to mobile phones and anchors such calls to the user desktop number. (Prior to the implementation of this feature, if an enterprise user made a direct call to a mobile phone, the call was treated like a normal outgoing PSTN call: the call got directed to the mobile phone only and the mobile user could not invoke any mobility features.)

An outgoing call from the enterprise to a remote destination exhibits the following behavior:

- Mobile user can use DTMF to invoke midcall features, such as Hold, Resume, Transfer, and Conference.
- Mobile user can hang up the call from the mobile phone and pick the call up from the user desk phone.
- A direct call to a remote destination from the enterprise gets anchored to the user desk phone; and the time-of-day access, Do Not Disturb, and Delay Before Ringing settings that are configured in the associated remote destination profile get ignored. The direct call goes immediately to the mobile user.
- Direct calls to remote destinations behave similarly to calls incoming to Cisco Unified Communications Manager from mobile users. Mobile users have access to the following mobility features:
  - Midcall features (Hold, Resume, Transfer, Conference)
  - Session Handoff
  - Call anchoring
Feature Configuration

Basic configuration of the Intelligent Session Control feature requires that the administrator configure the value of the Reroute Remote Destination Calls to Enterprise Number service parameter as True.

To access the service parameters in question, execute System > Service Parameters in Cisco Unified Communications Manager Administration. In the Service Parameter Configuration window that displays, specify a server and the Cisco CallManager service. The following service parameters are found in the Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number) pane:

- Reroute Remote Destination Calls to Enterprise Number—To enable the feature, specify the value for this service parameter as True. When this parameter is enabled, all outgoing calls to a remote destination get anchored in the enterprise number with which the remote destination associates.

- Log Mobile Number in CDR for Rerouted RD Calls—This service parameter determines whether to log the mobile number or the enterprise number in the call detail record (CDR) when outgoing calls to the remote destination get anchored. If set to False, the enterprise number gets logged. If set to True, the mobile number gets logged.

- Ignore Call Forward All on Enterprise DN—This service parameter determines whether to ignore the call forward all (CFA) setting that is configured on the enterprise number when outgoing calls to the remote destination get anchored. If set to True, the CFA gets ignored; if set to False, the CFA setting gets applied.

The following service parameters, found in the Clusterwide Parameters (System - Mobility) pane, also affect the behavior of the Intelligent Session Control feature:

- Matching Caller ID with Remote Destination—If this service parameter is set to Complete Match, all digits of the calling number must match for the call to connect to the remote destination. If this service parameter is set to Partial Match, partial matches are allowed and the Number of Digits for Caller ID Partial Match service parameter applies.

- Number of Digits for Caller ID Partial Match—The number of digits that this service parameter specifies applies to partial matches if the Matching Caller ID with Remote Destination service parameter is set to Partial Match.

Note

For each service parameter, click the service parameter name in Cisco Unified Communications Manager Administration for a complete definition of that service parameter.

Further Topics

This section includes the following topics:

- Additional Call Processing Details for Intelligent Session Control, page 14-18
- Use Case Scenarios for Intelligent Session Control, page 14-24
- Troubleshooting the Intelligent Session Control Feature, page 14-19

The “Use Case Scenarios for Intelligent Session Control” section on page 14-24 provides use case scenarios for the Intelligent Session Control feature with Cisco Unified Mobility.

Additional Call Processing Details for Intelligent Session Control

If more than one line is configured for the matching remote destination profile for the dialed number, Cisco Unified Communications Manager uses the first matched line to route the call. Because the direct call to mobile number gets matched against the enterprise number, all enterprise number intercepts are honored, including Call Intercept on enterprise number when Call Intercept gets supported for enterprise number. The forward all intercept on enterprise number gets ignored based on the service parameter,
Ignore Forward All on Enterprise DN. If this service parameter is set to true, Cisco Unified Communications Manager ignores forward all intercept on enterprise number and still directs the call to the mobile phone. If this service parameter is set to false, Cisco Unified Communications Manager still enables CFA setting on enterprise number and, if configured, sends the call to CFA destination. This feature does not anchor direct calls to mobile number if the call to mobile number gets sent via an overlap-sending-enabled trunk or gateway. In this case, the call to mobile number does not get anchored. See the “Limitations” section on page 14-30 for additional restrictions that apply to this feature.

Troubleshooting the Intelligent Session Control Feature
Perform the following checks if the Intelligent Session Control feature does not function as expected:

- Ensure that the Intelligent Session Control is set to True in the Service Parameter Configuration window.
- Ensure that the caller ID matches the remote destination number as specified by the Matching Caller ID with Remote Destination setting (either complete match or partial match).
- Ensure that a trace line such as the following prints in the Cisco Unified Communications Manager SSI log after the number gets dialed:
  
  10/14/2008 15:09:26.507 CCM|Digit analysis: getDaRes - Remote Destination [9725782583]|*^*^*

- Ensure that the enterprise number Line Association check box is checked in the Remote Destination Configuration window (Device > Remote Destination).
- Ensure that the route pattern partition is part of the calling search space (CSS) that is configured as Rerouting CSS in the Remote Destination Profile Configuration window (Device > Device Settings > Remote Destination Profile).

Additional Information
See the “Related Topics” section on page 14-62.

Session Handoff

The complete Session Handoff feature can move a single call, a conference, and session collaboration among mobile phone, PC, and desk phone. Session Handoff enables a user to move conversations from user mobile phone to user desk phone. Two-touch Session Handoff uses two user inputs: one at the initiating party to hand off and the other at the terminating party to accept.

The major benefit of the Session Handoff feature over Desktop Pickup is that the original conversation can be continued until the handed off call gets answered.

Configuration of Session Handoff Feature
Configuration of the Session Handoff feature entails configuration of specific service parameters and configuration of the mobile device that will hand off calls. See the following topics:

- Session Handoff Service Parameters, page 14-20
- Mobility Device Configuration for Session Handoff Feature, page 14-20
Session Handoff Service Parameters

To configure service parameters in Cisco Unified Communications Manager Administration, choose the System > Service Parameters menu option. From the Server drop-down list box, choose a server. From the Service drop-down list box, choose the Cisco CallManager service.

The following service parameters must be configured to enable the Session Handoff feature:

- **Session Handoff Alerting Timer**—This service parameter, found in the Clusterwide Parameters (Device - General) pane, determines the length of time that the session handoff call alerts. The default value specifies 10 seconds, and valid values range from 1 to 999 seconds.

- **Enterprise Feature Access Code for Session Handoff**—This service parameter, found in the Clusterwide Parameters (System - Mobility) pane, specifies the DTMF feature code to trigger session handoff. The default value specifies *74.

For additional details about these service parameters, click the name of the service parameter in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration, which provides a hyperlink to a complete definition of the service parameter.

Mobility Device Configuration for Session Handoff Feature

Perform the following configuration for the mobility device to enable the Session Handoff feature:

- Configure the directory number in remote destination profile and the desk phone shared line so that line-level directory number and partition match.

- Assign the same mobility user ID on the remote destination profile as the desk phone owner user ID to allow session handoff.

- To configure the Session Handoff feature for basic Cisco Unified Mobility users, the User ID field setting in the Remote Destination Configuration window should match the Owner User ID field on the (desk) phone configuration window.

- To configure the Session Handoff feature for Cisco Unified Mobile Communicator users, both the Owner User ID and the Mobility User ID fields in the Cisco Unified Mobile Communicator device configuration window must match the Owner User ID field on the desk phone configuration window.

Impact of Session Handoff on Other Features

When the user hands off a call, a new call gets presented on the desk phone. While the desk phone is flashing, the following features do not get triggered on the desk phone for the call that was handed off:

- iDivert

- Call Forward All

- DND

- Call Forwarding

If the user hands off a call and does not answer from the desk phone within the time that the Session Handoff Alerting Timer service parameter specifies, the existing Remote In Use state on the desk phone gets lost.

Thus, the desk phone loses shared-line functionality following session handoff. The user cannot perform midcall features for that call, such as Hold from Mobile (using *81) and Resume from desk, or desk pickup. The user can hand off the call again, however, to resume it from the desk phone.
Additional Topics for Session Handoff
See the following section for other topics that apply to the Session Handoff feature:

- Session Handoff Feature, page 14-34
- Use Case Scenarios for Session Handoff, page 14-26

Troubleshooting Information for Session Handoff Feature
If a call that is handed off from a mobile phone does not flash the desk phone, perform the following checks:

- Check whether Owner User ID for the desk phone matches the User ID of Remote Destination Profile.
- In service parameters, check whether Enable Enterprise Feature Access is set to True; also, check whether other DTMF features (Hold [*81], Resume [*83]) are working.
- Check the Session Handoff DTMF code (default specifies *74) and Session Handoff Alerting Timer (default specifies 10 seconds) values.

Additional Information
See the “Related Topics” section on page 14-62.

Use Case Scenarios for Cisco Unified Mobility Features

The following sections describe the following use case scenarios that Cisco Unified Communications Manager supports for Cisco Unified Mobility features:

- Use Case Scenarios for Mobile Connect, page 14-21
- Use Case Scenarios for Mobile Voice Access, page 14-22
- Use Case Scenarios for Time-of-Day Access, page 14-22
- Use Case Scenarios for Directed Call Park via DTMF, page 14-23
- Use Case Scenarios for Intelligent Session Control, page 14-24
- Use Case Scenarios for Session Handoff, page 14-26

Additional Information
See the “Related Topics” section on page 14-62.

Use Case Scenarios for Mobile Connect

Mobile Connect supports these use case scenarios:

- Receiving an outside call on desk phone or mobile phone—An outside caller dials the user desktop extension. The desk phone and mobile phone ring simultaneously. When the user answers one phone, the other phone stops ringing. The user can switch from the desk phone to a mobile phone during a call without losing the connection. Switching gets supported for incoming and outgoing calls.
- Moving back from a mobile phone to a desk phone—If a call was initiated to or from the desk phone and then shifted to the mobile phone, the call can get shifted back to the desk phone.
- Using midcall enterprise features—During a Mobile Connect call, users can perform midcall functions, including hold/resume, exclusive hold, transfer, directed call park, and conference.
Use Case Scenarios for Mobile Voice Access

Mobile Voice Access supports these use case scenarios:

- Initiating a mobility call from a remote phone, such as a mobile phone—Users can use Mobile Voice Access to initiate calls from a mobile phone as if dialing from the desk phone.
- Moving from a mobile phone to a desk phone during a mobile-phone-initiated call—If the user initiated a call from a mobile phone by using Mobile Voice Access, the user can shift to the desk phone during the call without losing the connection and can shift back again as needed.

Use Case Scenarios for Time-of-Day Access

The use case scenarios that follow detail the function of the time-of-day access feature with activated access lists that were configured prior to the addition of the time-of-day access feature; the use case scenarios also cover new provisioning that takes place for the feature starting with Release 7.0(1) of Cisco Unified Communications Manager.

Supported Use Cases for Migrating Activated Access Lists from an Earlier Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility when migration of an activated access list from a previous release of Cisco Unified Communications Manager to Release 7.0(x) or later takes place.

- **Use Case #1**—No allowed or blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.
  
  Result after migration: The system allows all calls at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Always ring this destination radio button is checked.

- **Use Case #2**—Only an allowed access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.
  
  Result after migration: Only the callers that belong to the allowed access list can reach the associated remote destination. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Ring this destination only if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.

- **Use Case #3**—Only a blocked access list got configured prior to Release 7.0(x) of Cisco Unified Communications Manager.
  
  Result after migration: The callers that belong to the blocked access list cannot reach the associated remote destination, but all other callers can call the remote destination at all hours. The Remote Destination Configuration window displays the When Mobile Connect is Enabled pane. In the Ring Schedule pane, the All the time radio button is checked. In the When Receiving a call during the above ring schedule pane, the Do not ring this destination if caller is in radio button is checked, and the access list displays in the corresponding drop-down list box.
Use Cases for Time-of-Day Access with the Current Cisco Unified Communications Manager Release

The following use cases detail the function of the Time-of-Day Access feature with Cisco Unified Mobility with the current release of Cisco Unified Communications Manager:

- **Use Case #4**—Only allow calls during business hours.
  
  **Configuration:** Configure a ring schedule that specifies business hours from Monday to Friday and choose the Always ring this destination radio button.
  
  **Result:** The system allows all callers during business hours, but no calls get extended to this remote destination outside business hours.

- **Use Case #5**—Only allow calls from certain numbers (for example, from coworkers) during business hours.
  
  **Configuration:** Configure a ring schedule that specifies business hours from Monday to Friday, choose the Ring this destination only if the caller is in radio button, and specify an access list.
  
  **Result:** Only callers that belong to the access list can call the remote destination during business hours; all other callers get blocked during business hours. Outside business hours, no calls ring this remote destination.

- **Use Case #6**—Block certain numbers (for example, 1800 numbers) during business hours.
  
  **Configuration:** Configure a ring schedule that specifies business hours from Monday to Friday, choose the Do not ring this destination if caller is in radio button, and specify an access list.
  
  **Result:** Only callers that belong to the access list get blocked from calling the remote destination during business hours; all other callers can call the remote destination during business hours. Outside business hours, no calls ring this remote destination.

**Additional Information**

See the “Related Topics” section on page 14-62.

Use Case Scenarios for Directed Call Park via DTMF

The Directed Call Park via DTMF feature of Cisco Unified Mobility supports the following use cases:

- Mobile phone user parks call on selected park code.
- Mobile phone user parks call on selected park code that is unavailable.
- Mobile phone user parks call on selected park code that is invalid.
- Mobile phone user fails to enter park code after entering the DTMF transfer code.
- Parked party disconnects while the parking party attempts to park the call.
- Parked party disconnects while it is parked on a selected park code and is waiting for retrieval.
- User dials Directed Call Park retrieval digits plus a park code that has not been occupied.
- Administrator configures a translation pattern, so the length of the string of digits to park a call and the length of the string to retrieve a call are the same.
- User retries a parked call.
- A parked call reverts.
- While a park code is occupied, one of the following entities gets modified or deleted: the park code or code range, the Directed Call Park park-prefix digits, or the Directed Call Park retrieval-prefix digits.
- Directed call park gets specified when the network is partitioned.
Use Case Scenarios for Intelligent Session Control

The Intelligent Session Control feature supports these use case scenarios:

- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
- The Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
- The Ignore Call Forward All on Enterprise DN service parameter is set to False.

The following sections discuss the configuration that takes place in order to demonstrate each user case for the Intelligent Session Control feature.

Use Case 1: Reroute Remote Destination Calls to Enterprise Number service parameter is set to False

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Route pattern points to the rcdn-gw gateway.

Figure 14-1 illustrates the setup for the direct call to the remote destination when the Reroute Remote Destination Calls to Enterprise Number service parameter is set to False.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. No remote destination mapping to enterprise number occurs.
5. The call extends only to the mobile user via the gateway; the call does not get anchored at the enterprise number with which this remote destination associates.

**Use Case 2: Reroute Remote Destination Calls to Enterprise Number service parameter is set to True**

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
3. Phone A DN specifies 5137000.
4. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583.
5. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
6. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
7. Route pattern points to the rcdn-gw gateway.

The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After the route pattern removes the leading (PreDot) 9, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets anchored at the enterprise number of the called user and the call extends to the user remote destination.
6. Phone B enters Remote In Use (RIU) state after the mobile user answers the call.

**Use Case 3: Ignore Call Forward All on Enterprise DN service parameter is set to False**

In this use case, the following configuration takes place prior to the placement of the direct call from Cisco Unified Communications Manager to the remote destination:

1. Reroute Remote Destination Calls to Enterprise Number service parameter is set to True.
2. Ignore Call Forward All on Enterprise DN service parameter is set to False.
3. Number of Digits for Caller ID Partial Match service parameter specifies 7 digits for partial match.
4. Phone A DN specifies 5137000.
5. Phone B DN specifies 5135282 with owner user ID gbuser1 and remote destination (RD) specifies 9725782583. Call Forward All setting for phone B specifies forwarding to phone C with DN 5138000.
6. Route pattern 9.XXXXXXXXXX with DDI as PreDot.
7. Translation pattern 0.XXXXXXX with DDI as PreDot and prefix digits specify 9972.
8. Route pattern points to the rcdn-gw gateway.
The following action initiates the feature behavior in this use case:

- Phone A DN 5137000 user calls the mobile phone by dialing 05782583.

The following call processing takes place:

1. The translation pattern gets matched and the called number gets transformed to 99725782583.
2. The route pattern 9.XXXXXXXXXX gets matched.
3. After transformation, the number specifies 9725782583.
4. Remote destination mapping to enterprise number matches the configured remote destination for phone B.
5. The call gets redirected to the enterprise number of the user and goes to phone B instead of to the mobile phone.
6. Because of the setting of the Ignore Call Forward All on Enterprise DN service parameter to False, the call gets forwarded from phone B to phone C.

Additional Information
See the “Related Topics” section on page 14-62.

Use Case Scenarios for Session Handoff

The Session Handoff feature supports the following use case scenarios:

- Session Handoff using DTMF Tones (*74)
- Session Handoff using Move Softkey Event
- Session Handoff using VoIP Mode
- Session Handoff Fails or User Cancels Session Handoff

Session Handoff Using DTMF Tones (*74)
For session handoff using DTMF tones (default specifies *74), the following sequence of events takes place:

1. User A calls user B desk phone. Using the Single Number Reach feature, user B answers the call on mobile phone and his desk phone goes into Remote In Use state.
2. User B presses *74 (Session Handoff DTMF code). User B desk phone (a supported phone that is running SCCP or SIP) flashes. User B still talks with user A from user B mobile phone.
3. To move conversation to the desk phone, user B must answer the call from desk phone before the Session Handoff Alerting Timer service parameter (default 10s) expires. After the timer expires, the desk phone stops flashing. User B can still continue conversation from the mobile phone.

Session Handoff Using Move Softkey Event
For session handoff using the Move softkey event, the following sequence of events takes place:

1. Session Handoff gets triggered by using a Move softkey event message that gets embedded inside the SIP REFER message.
2. When Cisco Unified Communications Manager receives the REFER message, Cisco Unified Communications Manager triggers session handoff.
If user mobile device disconnects a call for which Session Handoff has been initiated, the call can still be continued by resuming the call at the desk phone prior to the expiration of the Session Handoff Alerting Timer. These cases can occur when a user moves to an area that does not have mobile connectivity, such as an elevator or dead zone/spot.

**Session Handoff Using VoIP Mode With SIP Clients**

For SIP clients, session handoff support exists for VoIP mode as well as for cellular mode. For this scenario, the following steps take place:

1. User that is using a SIP client on a remote destination in VoIP (Wi-Fi) mode initiates session handoff by using the Move softkey on the smartphone.
2. Cisco Unified Communications Manager flashes the shared line on the desk phone and does not break media until the desk phone answers the call.

Be aware that this function also works if the user is logged on to extension mobility.

**Session Handoff Fails or User Cancels Session Handoff**

If session handoff fails, the following steps take place:

1. Cisco Unified Mobile Communicator or a VoIP client initiates session handoff to a station that does not have the correct owner user ID.
2. Session handoff fails. A “Cannot move conversation” SIP message gets sent to the client.

If the user cancels session handoff, the session handoff stops. The following steps take place:

1. The user initiates session handoff from Cisco Unified Mobile Communicator or a VoIP client.
2. Before the session handoff completes, the user cancels the session handoff from the client.
3. Cisco Unified Communications Manager cancels the session handoff. Shared-line devices stop ringing.

**Additional Information**

See the “Related Topics” section on page 14-62.

**Interactions and Limitations**

Most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features, except as indicated in the following sections:

- Interactions, page 14-28
- Limitations, page 14-30

**Additional Information**

See the “Related Topics” section on page 14-62.
Interactions

The following topics detail the interactions between Cisco Unified Mobility and other Cisco Unified Communications Manager components:

- Auto Call Pickup, page 14-28
- Automatic Alternate Routing, page 14-28
- External Call Control, page 14-29
- Intelligent Session Control and Session Handoff, page 14-29
- Licensing, page 14-29
- Local Route Groups, page 14-29
- Mobile Connect and SIP Trunks With Cisco Unified Border Element, page 14-30
- Number of Supported Calls, page 14-30

Auto Call Pickup
Cisco Unified Mobility interacts with auto call pickup based on the service parameter selection. When the Auto Call Pickup Enabled service parameter is set to True, end users need only to press the PickUp softkey to pick up a call.

If the Auto Call Pickup Enabled service parameter is set to False, end users need to press the PickUp, GPickUp, or OPickUp softkey and then the Answer softkey.

Auto Call Pickup Example
Phone A, phone B (Cisco Unified Mobility subscriber), and phone C belong to the Engineering group; phone D, phone E, and phone F belong to the Accounting group.

Phone D calls phone A in the Engineering Group. Phone A rings, and phone B and phone C in the group receive pickup notice.

If Auto Call Pickup is enabled, press the PickUp softkey from phone B to use Cisco Unified Mobility features later on.

If Auto Call Pickup is not enabled, press PickUp softkey from phone B, which causes the remote destinations that are associated with phone B to ring. Press the Answer softkey on phone B, which causes the remote destinations to stop ringing. The user can subsequently perform mobile-phone pickup and desktop call pickup.

Automatic Alternate Routing
Prior to the implementation of this interaction, if a desk phone was configured for Automatic Alternate Routing (AAR) and the desk phone was configured with a mobile phone as a remote destination, the AAR feature did not get triggered for calls to the remote destination if the out-of-bandwidth condition applied.

Cisco Unified Mobility now supports Automatic Alternate Routing (AAR) as follows:

- If a rejection occurs due to lack of bandwidth for the location-based service, the rejection triggers AAR for any device that is configured for AAR.
- If a rejection occurs based on Resource Reservation Protocol (RSVP), however, AAR does not get triggered for calls to remote destinations.
External Call Control

If external call control is configured, as described in the “External Call Control” chapter, Cisco Unified Communications Manager honors the route decision from the adjunct route server for the following Cisco Unified Mobility features:

- Mobile Connect
- Mobile Voice Access
- Enterprise Feature Access
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward

To invoke Mobile Voice Access or Enterprise Feature Access, the end user must dial a feature directory number that is configured in Cisco Unified Communications Manager Administration. When the Cisco Unified Communications Manager receives the call, Cisco Unified Communications Manager does not invoke external call control because the called number, in this case, is the feature DN. After the call is anchored, the Cisco Unified Communications Manager asks for user authentication, and the user enters the number for the target party. When Cisco Unified Communications Manager tries to extend the call to the target party, external call control gets invoked, and Cisco Unified Communications Manager sends a call routing query to the adjunct route server to determine how to handle the call.

Cisco Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features:

- Cell pickup
- Desk pickup
- Session handoff

Intelligent Session Control and Session Handoff

For direct calls to remote destinations that get anchored to the enterprise number, the mobile user can invoke the Session Handoff feature and mobile user can hand off the call to the desk phone.

Licensing

Mobile Connect uses licensing. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units (DLUs) for Mobile Connect; the number of licenses that get consumed depends on whether you assign an adjunct device to the end user specifically for Cisco Unified Mobility. For specific information on how licensing works with Cisco Unified Mobility, see the following sections:

- “Licenses for Cisco Unified Mobility” in the Cisco Unified Communications Manager Features and Services Guide
- “Cisco Unified Mobility for End Users” in the Cisco Unified Communications Manager System Guide

Local Route Groups

For Single Number Reach calls to a remote destination, the device pool of the originating calling party determines the selection of the Standard Local Route Group.
Mobile Connect and SIP Trunks With Cisco Unified Border Element
Cisco Unified Mobility supports the Mobile Connect feature without midcall features over SIP trunks with Cisco Unified Border Element (CUBE).

Number of Supported Calls
Each remote destination supports a maximum of two active calls. For Cisco Unified Mobility, each remote destination supports a maximum of two active calls via Cisco Unified Communications Manager. Using the Enterprise Feature Access directory number (DID number) to transfer or conference with DTMF counts as one call. When a Cisco Unified Mobility user receives a call while the user has two active calls for the remote destination or while the user is using DTMF to transfer/conference a call from the remote destination, the received call does not reach the remote destination and instead goes to the enterprise voice mail; that is, if Call Forward No Answer (CFNA) is configured or if the call is not answered on a shared line.

Additional Information
See the “Related Topics” section on page 14-62.

Limitations
Cisco Unified Mobility enforces the following limitations in operating with other Cisco Unified Communications Manager components:

- Call Anchoring, page 14-31
- Call Forwarding, page 14-31
- Cisco Unified IP Phones 7940 and 7960 That Are Running SIP, page 14-31
- Conferencing, page 14-31
- Dialing + Character From Mobile Phones, page 14-31
- DND on the Desk Phone and Direct Calls to Remote Destination, page 14-32
- Dual-Mode Handoff and Caller ID, page 14-32
- Dual-Mode Phones and Call Anchoring, page 14-32
- Dual-Mode Phones and CTI Applications, page 14-32
- Dual-Mode Phones and Desktop Call Pickup, page 14-32
- Dual-Mode Phones That Are Running SIP and Registration Period, page 14-32
- Enterprise Features From Cellular Networks, page 14-32
- Enterprise Features in GSM That Is Using DTMF, page 14-33
- Gateways and Ports, page 14-33
- Maximum Wait Timer for Desktop Call Pickup Does Not Get Applied If Hold DTMF Is Pressed, page 14-33
- Mobile Connect Support Restrictions, page 14-33
- Multilevel Precedence and Preemption (MLPP), page 14-33
- Multiple-Node Cluster Environment, page 14-33
- Overlap Sending, page 14-33
Call Anchoring
Call anchoring, which is performed based on caller ID, gets supported only from calls from registered single-mode or dual-mode phones.

Call Forwarding
You do not need to configure settings for call forward unregistered, if the end user has configured remote destinations. Appropriate call forwarding will get handled as part of the Mobile Connect process.

Cisco Unified IP Phones 7940 and 7960 That Are Running SIP
When running SIP, Cisco Unified IP Phones 7940 and 7960 do not support the Remote-in-use state and therefore cannot support desktop call pickup.

For these phones, if the mobile phone user hangs up a call that the Cisco Unified IP Phone 7940 or 7960 that is running SIP extended to the mobile phone, the calling party hears music on hold for ten seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote destination end user) and then the call drops. Because the desktop call pickup feature does not get supported for these phones when they are running as SIP devices, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

Cisco recommends that you configure Cisco Unified IP Phones 7940 and 7960 to run SCCP for users that are enabled for Cisco Unified Mobility.

Conferencing
Users cannot initiate a meet-me conference as conference controller by using Mobile Voice Access but can join a meet-me conference.

If an existing conference call is initiated from a shared-line IP phone or dual-mode phone or smartphone that is a remote destination, no new conference party can get added to the existing conference after the call is sent to a mobile phone or a dual-mode handoff action occurs. To permit the addition of new conference parties, use the Advanced Ad Hoc Conference Enabled service parameter.

Dialing + Character From Mobile Phones
Users can dial a + sign through DTMF on a mobile phone to specify the international escape character. Cisco Unified Mobility does not support + dialing through DTMF for interactive voice response (IVR) to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character.

Cisco Unified Mobility does not support + dialing through DTMF for two-stage dialing to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character.
For more information about configuring the international escape character in Cisco Unified Communications Manager Administration, see the “Using the International Escape Character +” section in the Cisco Unified Communications Manager System Guide.

**DND on the Desk Phone and Direct Calls to Remote Destination**

If Do Not Disturb (DND) is enabled on a desk phone, the desk phone cannot be placed in the Remote In Use (RIU) state and the call does not get anchored in these cases:

- DND is enabled with the call reject option—The call cannot get anchored.
- DND is activated by pressing the DND softkey on the desk phone—The call cannot get anchored.

If DND is enabled with the ring off option, however, the call does get anchored.

**Dual-Mode Handoff and Caller ID**

Dual-mode handoff requires that caller ID be available in the cellular network.

**Dual-Mode Phones and Call Anchoring**

Dual-mode phones (Cisco Unified Mobility Advantage and dual-mode phones that are running SCCP or SIP) that are configured as remote destinations cannot anchor calls.

**Dual-Mode Phones and CTI Applications**

While a dual-mode phone is in Wi-Fi enterprise mode, no CTI applications control it nor monitor it.

The In Use Remote indicator for dual-mode phones on a shared line call in the WLAN disappear if the dual-mode phone goes out of WLAN range.

**Dual-Mode Phones and Desktop Call Pickup**

The desktop call pickup feature does not apply to the following mobile phone models:

- Nokia 902iL and Nokia 906iL dual-mode phones that are running SIP
- Nokia S60 dual-mode phones that are running SCCP

For these phone models, if the mobile phone user hangs up a call, the calling party hears music on hold for ten seconds (as configured by the Maximum Wait Time for Desk Pickup field for the remote destination end user) and then the call drops. Because the desktop call pickup feature does not get supported for these phone models, the user desk phone does not display the Resume softkey, so the user cannot pick up the call on the desk phone.

**Dual-Mode Phones That Are Running SIP and Registration Period**

For dual-mode phones that are running SIP, Cisco Unified Communications Manager determines the registration period by using the value in the Timer Register Expires (seconds) field of the SIP profile that associates with the phone, not the value that the SIP Station KeepAlive Interval service parameter specifies.

**Enterprise Features From Cellular Networks**

Enterprise features from cellular networks require out-of-band DTMF.

---

**Note**

When using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check the Require DTMF Reception check box when configuring the IP phone, so DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.
Enterprise Features in GSM That Is Using DTMF
Availability of enterprise features in GSM that is using DTMF depends upon the features that are supported in the third-party smartphones.


The Forced Authorization Code (FAC) does not get invoked for Mobile Connect [Single Number Reach (SNR)] calls to a remote destination.

Gateways and Ports
Both H.323 and SIP VoIP gateways get supported for Mobile Voice Access.
Mobile Connect features do not get supported for T1 CAS, FXO, FXS and BRI.

Maximum Wait Timer for Desktop Call Pickup Does Not Get Applied If Hold DTMF Is Pressed
If a user presses the *81 DTMF code from a remote destination (either a smartphone or any other phone) to put a call on hold, the user desk phone displays the Resume softkey. The desk phone does not apply a timer for desktop call pickup, however; the Resume key does not stop displaying after the timeout that is configured for the end user to pick up the call and the call does not get dropped.

Instead, users should hang up the call on the remote phone, which triggers the desk phone to apply the timer for desktop call pickup. (Use the Maximum Wait Time for Desk Pickup field on the End User Configuration window to change this setting.)

Mobile Connect Support Restrictions
The Mobile Connect feature gets supported only for Primary Rate Interface (PRI) public switched telephone network (PSTN) connections.

For SIP trunks, Mobile Connect gets supported via IOS gateways or intercluster trunks.

Multilevel Precedence and Preemption (MLPP)
Mobile Connect does not work with Multilevel Precedence and Preemption (MLPP). If a call is preempted with MLPP, Mobile Connect features get disabled for that call.

Multiple-Node Cluster Environment
In a multiple-node cluster environment, if the Cisco Unified Communications Manager publisher server is unreachable, any changes that end users make to turn Mobile Connect off or on by way of Mobile Voice Access or two-stage dialing do not get saved.

Overlap Sending
Overlap sending patterns do not get supported for the Intelligent Session Control feature.

QSIG Path Replacement
QSIG (Q Signaling) path replacement does not get supported.

Remote Destination Profiles
When configuring a directory number that is associated with a remote destination profile, you must use only ASCII characters in the Display (Internal Caller ID) field on the Directory Number Configuration window.
Remote Destinations
Ensure remote destinations are Time Division Multiplex (TDM) devices. You cannot configure IP phones within a Cisco Unified Communications Manager cluster as remote destinations.
Ensure remote destinations specify PSTN numbers or numbers across ICT trunks.
Remote destinations cannot resume calls that Cisco Unified IP Phones put on hold.

Service Parameters
Enterprise feature access service parameters apply to standard phones and smartphones; however, smartphones generally use one-touch keys to send the appropriate codes. Administrators must configure any smartphones that will be used with Mobile Connect to use either the default codes for enterprise feature access or the codes that are specified in the smartphone documentation.

Session Handoff Feature
The following limitations apply to the Session Handoff feature:
- Session Handoff can take place only from mobile phone to desk phone. For the other direction, the current Remote Destination Pickup method specifies using Send Call to Mobile Phone.
- Only audio call session handoff gets supported.

SIP URI and Direct Calls to Remote Destination
The Intelligent Session Control feature does not support direct URI dialing. Therefore, calls made to a SIP URI cannot be anchored to an enterprise number.

Video Calls
Mobile Connect services do not extend to video calls. A video call that is received at the desk phone cannot get picked up on the mobile phone.

Additional Information
See the “Related Topics” section on page 14-62.

System Requirements
Mobile Connect and Mobile Voice Access require the following software components:
- Cisco Unified Communications Manager 6.0 or later.
- Cisco Unified Mobile Voice Access service, which runs only on the publisher.
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones).
To see which IP phones work with Mobile Connect and Mobile Voice Access, see the applicable Cisco Unified IP Phone Administration Guide and Cisco Unified IP Phone User Guide.

Additional Information
See the “Related Topics” section on page 14-62.
Migrating from Cisco Unified MobilityManager

Follow this process to migrate standalone Cisco Unified MobilityManager data to Cisco Unified Communications Manager:

1. Upgrade the Cisco Unified MobilityManager system to Release 1.2(5), if necessary. See the Release Notes for Cisco Unified MobilityManager Release 1.2(5).

2. Log in to Cisco Unified MobilityManager and export the configuration data in CSV format. For instructions, see the Release Notes for Cisco Unified MobilityManager Release 1.2(5).

3. Log in to Cisco Unified Communications Manager Administration and use the Bulk Administration Import/Export windows to import the CSV data files that were previously exported from Cisco Unified MobilityManager. See the “Access List,” “Remote Destination,” and “Remote Destination Profile” chapters in the Cisco Unified Communications Manager Bulk Administration Guide.

Additional Information
See the “Related Topics” section on page 14-62.

Configuring Cisco Unified Mobility

This section provides detailed procedures for each Cisco Unified Communications Manager Administration menu option that must be configured to provision Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

See the “Configuration Checklist for Cisco Unified Mobility” section on page 14-2 for an overview checklist of the procedures and steps that are necessary for an administrator to configure Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

End users use the Cisco Unified CM User Options windows to further configure or modify the Cisco Unified Mobility settings that apply to their mobile phones.

This section covers the following topics:

- Access List Configuration, page 14-36
- Remote Destination Profile Configuration, page 14-39
- Remote Destination Configuration, page 14-43
- Mobile Voice Access Directory Number Configuration, page 14-48
- Gateway Configuration for Enterprise Feature Access, page 14-50
- Enterprise Feature Access Two-Stage Dialing, page 14-55
- Mobility Enterprise Feature Configuration, page 14-56
- Handoff Mobility Configuration, page 14-57
- Mobility Profile Configuration, page 14-58
- Mobility Softkey Configuration, page 14-61

Tip
Before you configure Cisco Unified Mobility, review the “Configuration Checklist for Cisco Unified Mobility” section on page 14-2.
Access List Configuration

You can define access lists to explicitly allow or block the extension of Mobile Connect calls to remote destinations based on the caller ID of the caller.

To configure access lists, see the following sections:

- Access List Configuration Settings, page 14-36
- Access List Member Detail Configuration Settings, page 14-38

Additional Information
See the “Related Topics” section on page 14-62.

Access List Configuration Settings

In Cisco Unified Communications Manager Administration, use the Call Routing > Class of Control > Access List menu path to configure access lists.

An access list, which supports Cisco Unified Mobility, specifies a list that determines the phone numbers that the system can pass or block from being passed to remote destinations. For more information on Cisco Unified Mobility, See the “Related Topics” section on page 14-62.

Tips About Configuring Access Lists
While you configure an access list, follow these additional steps to configure its members:

**Step 1**
If you want to configure the members of an access list, click Add Member and enter values for the parameters that are described in Table 14-5.

**Step 2**
Click Save.

The Access List Configuration window reopens to show the new number or filter in the Selected Filters area.

**Step 3**
From the Access List Configuration window, add additional filters and also modify any existing access list as needed:

- To modify a DN mask, click the link for the directory number at the bottom of the window under Access List Members, enter your change, and click Save.
- To delete a filter, select the filter and click Delete.
- To inactivate a filter without deleting it, select the filter in the Selected Filters pane and click the down arrow to move the filter to the Removed Filters pane.
- To activate a filter, select the filter in the Removed Filters pane and click the up arrow to move the filter to the Selected filters area.
- To create a new access list with the same members as the existing list, click Copy.
Tips About Deleting Access Lists

You cannot delete access lists that remote destinations are using. To find out which items are using the access list, choose Dependency Records from the Related Links drop-down list box that is on the Access List Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2 of the Cisco Unified Communications Manager Administration Guide. If you try to delete an access list that is in use, Cisco Unified Communications Manager displays a message. Before deleting an access list that is currently in use, you must perform either or both of the following tasks:

• Assign a different access list to any remote destinations that are using the access list that you want to delete. See the “Remote Destination Configuration” section on page 14-43.

• Delete the remote destinations that are using the access list that you want to delete. See the “Remote Destination Configuration” section on page 14-43.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-4 describes the available settings in the Access List Configuration window. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access List Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name (between 1 and 50 characters) for this access list. You may use all characters except quotes (&quot;), close angle bracket (&gt;), open angle bracket (&lt;), backslash (), ampersand (&amp;), and percent sign (%).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a text description (between 1 and 128 characters) for this access list. You may use all characters except nonprinting characters, such as tabs and quotes (&quot;).</td>
</tr>
<tr>
<td>Owner</td>
<td>From the drop-down list box, choose the end user to whom the access list applies.</td>
</tr>
<tr>
<td>Allowed</td>
<td>Click this radio button to allow calls from member phone numbers to be passed to the remote destinations.</td>
</tr>
<tr>
<td>Blocked</td>
<td>Click this radio button to block calls from member phone numbers from being passed to the remote destinations.</td>
</tr>
</tbody>
</table>
Additional Information

See the “Related Topics” section on page 14-62.

Access List Member Detail Configuration Settings

The Access List Member Detail window displays when you click the Add Member button on the Access List Configuration window while you configure an access list. The Access List Member Detail window allows you to configure the following settings for an access list member:

- Filter Mask
- DN Mask

After you configure a new access list member, the new access list member displays in the Access List Members pane at the bottom of the corresponding Access List Configuration window. You can click one of the access list members to view or change the settings for that access list member. To exit the Access List Member Detail window without making any changes, choose Back to Find/List from the Related Links drop-down list box and click Go.

Table 14-5 describes the available settings in the Access List Member Detail window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Mask</td>
<td>Select an option from the drop-down list box. You can choose to enter a directory number, filter out calls that do not have caller ID (Not Available), or specify a number that will be allowed or blocked without displaying the caller ID (Private).</td>
</tr>
</tbody>
</table>
Remote Destination Profile Configuration Settings

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Remote Destination Profile menu path to configure remote destination profiles.

Remote destination profiles, which support Cisco Unified Mobility, specify a set of parameters that apply to all remote destinations for the user. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

Tips About Configuring Remote Destination Profiles

The remote destination profile contains the parameters that apply to all remote destinations for the user. After configuring user accounts for Mobile Connect (see the “End User Configuration” chapter in the Cisco Unified Communications Manager Administration Guide), you can create a remote destination profile for the user.

Table 14-5  Access List Member Detail Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| DN Mask    | If you chose Directory Number in the Filter Mask field, enter a phone number or filter in the DN Mask field. You can use the following wild cards to define a filter:  
  • X (upper or lower case)—Matches a single digit.  
  • !—Matches any number of digits.  
  • #—Used as a single digit for exact match.  
Examples:  
  • 408! matches any number that starts with 408.  
  • 408555123X matches any number between 4085551230 and 4085551239.  
Note  
If you want to filter an incoming call from a calling number that begins with a leading +, you must include the leading + in the DN Mask field unless any supported wild card precedes the directory number. For example, if an end user wants to block +14081239876, the user access list needs to include either +14081239876 or !14081239876 in the DN Mask field. |
**Tips About Deleting Remote Destination Profiles**

You can delete remote destination profiles that associate with remote destinations. You receive a warning message that you are about to delete both a remote destination profile and the associated remote destinations.

To find out which items are using the remote destination profiles, choose **Dependency Records** from the Related Links drop-down list box that is on the Remote Destination Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2 of the *Cisco Unified Communications Manager Administration Guide*.

**Using the GUI**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration Settings Table**

(Table 14-6) describes the available settings in the Remote Destination Profile Configuration window. For related procedures, see the “Related Topics” section on page 14-62.

**Table 14-6 Remote Destination Profile Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a text name for the remote destination profile. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a text description of the remote destination profile. This field can comprise up to 128 characters. You can use all characters except quotes (&quot;), close angle bracket (&gt;), open angle bracket (&lt;), backslash (), ampersand (&amp;), and percent sign (%).</td>
</tr>
<tr>
<td>User ID</td>
<td>Choose the user to whom this profile is assigned. The selection must match the ID of a user in the End User Configuration window where Enable Mobility is checked.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose the device pool that applies to this profile. The device pool defines sets of common characteristics for devices, such as region, date/time group, softkey template, and MLPP information.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>Choose the calling search space to be used for routing Mobile Voice Access or Enterprise Feature Access calls. <strong>Note</strong> This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls.</td>
</tr>
<tr>
<td>User Hold Audio Source</td>
<td>Choose the audio option for users on hold for Mobile Connect and Mobile Voice Access calls.</td>
</tr>
</tbody>
</table>
### Table 14-6 Remote Destination Profile Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>Choose the audio source from the IOS gateway that provides multicasting audio source for Mobile Connect and Mobile Voice Access calls.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Choose a privacy option for the remote destination profile. If you choose the Default value for this field, the setting matches the value of the Privacy Setting service parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you change and save the value of the Privacy Setting service parameter, you must return to the Remote Destination Profile Configuration window for a remote destination profile that specifies Default and click <strong>Save</strong> for the service parameter change to take effect.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot transfer a call from a cell phone to a desk phone if the Remote Destination Profile Privacy specifies On, and the “Enforce Privacy Setting on Held Calls” service parameter specifies True.</td>
</tr>
<tr>
<td></td>
<td>For more configuration information, see Barge and Privacy.</td>
</tr>
<tr>
<td>Rerouting Calling Search Space</td>
<td>Choose a calling search space to be used to route Mobile Connect calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Ensure that the gateway that is configured for routing mobile calls is assigned to the partition that belongs to the Rerouting Calling Search Space. Cisco Unified Communications Manager determines how to route calls based on the remote destination number and the Rerouting Calling Search Space.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Rerouting Calling Search Space setting applies only when you are routing calls to the remote destination or mobility identity, which specifies the outbound call leg toward the remote destination or mobility identity when a call comes in to the user enterprise number.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Mobile Connect calls do not get routed to the dual-mode mobility identity number that corresponds to the dual-mode mobile phone number if the device associates with the enterprise WLAN and registers with Cisco Unified Communications Manager. Mobile Connect calls get routed to the dual-mode mobility identity number only when the device is outside the enterprise.</td>
</tr>
</tbody>
</table>
Chapter 14  Cisco Unified Mobility

Configuring Cisco Unified Mobility

Calling Party Transformation

Choose the calling search space for transformations. This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Note**
The partitions in the calling search space should contain only calling party transformations.

**Note**
Ensure the calling search space is not null because no transformations can apply to null partitions.

**Note**
The device takes on the attributes of the Calling Party Transformation Pattern because you assign the pattern to a partition where the Calling Party Transformation CSS exists. For example, when you configure the Calling Party Transformation CSS under Call Routing > Class of Control > Calling Search Space, you assign the CSS to a partition; when you configure the Calling Party Transformation CSS under Call Routing > Transformation Pattern > Calling Party Transformation Pattern, you choose the partition where the Calling Party Transformation CSS is assigned.

Use Device Pool Calling Party Transformation CSS

To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Remote Destination Profile Configuration window.

User Locale

From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users.

Cisco Unified Communications Manager makes this field available only for phone models that support localization.

**Note**
If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before you configure user locale. See the Cisco Unified Communications Manager Locale Installer documentation.

Ignore presentation indicators (internal calls only)

Check the check box if you want to ignore the connected line ID presentation. Use this configuration for internal calls.

Associated Remote Destinations

Add a New Remote Destination

Click this link to open the Remote Destination Configuration window, where you can configure a new remote destination to associate with this remote destination profile. By default, the current remote destination profile is selected in the Remote Destination Profile field of the new remote destination. See the “Remote Destination Configuration” section on page 14-43 for details.
Chapter 14  Cisco Unified Mobility

Configuring Cisco Unified Mobility

**Table 14-6**  Remote Destination Profile Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>For a remote destination that already exists and has been associated with this remote destination profile, this column displays the name of the remote destination.</td>
</tr>
<tr>
<td>Destination Number</td>
<td>For a remote destination that already exists and has been associated with this remote destination profile, this column displays the destination number of the remote destination.</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Check this check box to enable Do Not Disturb on the phone.</td>
</tr>
<tr>
<td>DND Option</td>
<td>This Call Reject option specifies that no incoming call information gets presented to the user.</td>
</tr>
<tr>
<td>Note</td>
<td>For mobile devices, dual-mode phones, and phones that are running SCCP, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 14-62.

**Associating a Directory Number with a Remote Destination Profile**

After creating a remote destination profile, you must associate the DN record for the desk phone or phones for the user. Click the Add a New DN link on the Remote Destination Profile Configuration window and follow the instructions in the “Directory Number Configuration” chapter of the *Cisco Unified Communications Manager Administration Guide*.

**Note**

If the remote destination profile is dissociated on the Directory Number configuration window, you must check the Line Association check box for the DN on the Remote Destination window to reassociate it.

Additional Information

See the “Related Topics” section on page 14-62.

**Remote Destination Configuration**

After remote destination profiles and access lists are created, you can enter individual remote destinations and assign each to a profile. Each remote destination represents a mobile or other phone that can be configured to perform remote destination pickup (accept transfers from the desk phone of the user) and accept incoming Mobile Connect calls that come from the system as a result of the line that is shared with the desk phone.

After you save a new remote destination, the Association Information pane displays in the window. This section lists the desk phone numbers that have been assigned to the remote destination profile. You can click a link to open the associated Directory Number Information window. See “Directory Number Configuration Settings” in the *Cisco Unified Communications Manager Administration Guide*. 
This section describes how to access remote destination records by opening the Remote Destination Configuration window. You can also open an existing or new record in the Remote Destination Profile Configuration window by clicking the Add a New Remote Destination link at the bottom of the remote destination profile. See the “Remote Destination Profile Configuration” section on page 14-39 for instructions on displaying a remote destination profile.

To configure remote destinations, see the following section:
- Remote Destination Configuration Settings, page 14-44

Additional Information
See the “Related Topics” section on page 14-62.

Remote Destination Configuration Settings

In Cisco Unified Communications Manager Administration, use the Device > Remote Destination menu path to configure remote destinations.

Remote destinations represent phones that are available for Mobile Connect answer and pickup, plus locations that are used to reach Mobile Voice Access. Remote destinations may include any of the following devices:
- Single-mode mobile (cellular) phones
- Smartphones
- Dual-mode phones
- Enterprise IP phones that are not in the same cluster as the desk phone
- Home phone numbers in the PSTN.

For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

Tips About Configuring Remote Destinations

End users can create their own remote destinations in the Cisco Unified CM User Options windows. For information on how to perform this task, see the user guide for the phone model.

Be aware that the appropriate timer settings in Table 14-7 may be service-provider-specific. If difficulties in transferring calls by using the default timer settings occur, you may need to adjust the settings to be compatible with the service provider for the remote destination phone.

Check the Line Association check boxes for the desk phones that will be used with this remote destination. You must perform this step for Mobile Connect to work.

Note
This step requires that a directory number has already been configured on the remote destination profile with which the remote destination associates.

Tips About Deleting Remote Destinations

To find out which items are using the remote destination, choose Dependency Records from the Related Links drop-down list box that is on the Remote Destination Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2 of the Cisco Unified Communications Manager Administration Guide.
Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-7 describes the available settings in the Remote Destination Configuration window. For related procedures, see the “Related Topics” section on page 14-62.

Table 14-7 Remote Destination Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Destination Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name that identifies the remote destination or mobile identity.</td>
</tr>
<tr>
<td>Destination Number</td>
<td>Enter the telephone number for the destination. Include the area code and any additional digits that are required to obtain an outside line. Maximum field length equals 24 characters; individual characters can take the values 0-9, *, #, and +. Cisco recommends that you configure the caller ID of the remote destination.</td>
</tr>
<tr>
<td></td>
<td>Note Add the necessary translation pattern or route patterns to route the destination number.</td>
</tr>
<tr>
<td></td>
<td>For the SIP URI feature, you can also enter a Universal Resource Indicator (URI) in this field, such as <a href="mailto:user@corporation.com">user@corporation.com</a>, up to 126 characters in length. Keep in mind that a SIP route pattern must also be configured.</td>
</tr>
<tr>
<td></td>
<td>If the administrator configures the Incoming Calling Party settings in the Cisco Unified Communications Manager gateway, trunk, or device pool to globalize the incoming calling party number, configure the Destination Number of the remote destination in the E.164 format.</td>
</tr>
<tr>
<td></td>
<td>Example: For a remote destination with US area code 408 and destination number 5552222, configure the Destination Number as +14085552222.</td>
</tr>
<tr>
<td></td>
<td>Additionally, if globalized destination numbers are in use, set the Matching Caller ID with Remote Destination service parameter to Complete Match.</td>
</tr>
<tr>
<td>Answer Too Soon Timer</td>
<td>Enter the minimum time in milliseconds that Cisco Unified Communications Manager requires the mobile phone to ring before answering the call. This setting accounts for situations where the mobile phone is switched off or is not reachable, in which case the network may immediately divert the call to the mobile phone voice mail. If the mobile phone is answered before this timer expires, Cisco Unified Communications Manager pulls the call back to the enterprise.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 - 10,000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>Default: 1,500 milliseconds</td>
</tr>
</tbody>
</table>
Table 14-7 Remote Destination Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Too Late Timer</td>
<td>Enter the maximum time in milliseconds that Cisco Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Cisco Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise. Range: 10,000 - 300,000 milliseconds Default: 19,000 milliseconds</td>
</tr>
<tr>
<td>Delay Before Ringing Timer</td>
<td>Enter the time that elapses before the mobile phone rings when a call is extended to the remote destination. Range: 0 - 30,000 milliseconds Default: 4,000 milliseconds Tip When a hunt group is in use, the lines ring only for a short period of time. You may need to manipulate the Delay Before Ringing Timer setting and make it zero to allow a remote destination call to be established, ring, and answer, before the hunt list timer expires and pulls the call back.</td>
</tr>
<tr>
<td>Remote Destination Profile</td>
<td>From the drop-down list box, choose the remote destination profile that you want to use for this remote destination.</td>
</tr>
<tr>
<td>Mobility Profile</td>
<td>From the drop-down list box, choose the mobility profile that you want to use for this remote destination. To configure a mobility profile, use the Call Routing &gt; Mobility &gt; Mobility Profile menu option. See the “Mobility Profile Configuration” section on page 14-58 for details.</td>
</tr>
<tr>
<td>Cisco Unified Mobile Communicator</td>
<td>This field displays the Cisco Unified Mobile Communicator device with which this Mobility Identity associates. Click the Configure Device link to display the Phone Configuration window, where you can change the settings of the specified device.</td>
</tr>
<tr>
<td>Dual Mode Phone</td>
<td>This field displays a dual-mode phone with which this Mobility Identity associates. The field displays the device name. Click the Configure Device link to display the Phone Configuration window, where you can change the settings of the specified device.</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>Check the check box if you want calls that the desk phone answers to be sent to your mobile phone as the remote destination. Checking this check box ensures that, if Send Call to Mobile Phone is specified (by using the Mobility softkey for remote destination pickup), the call gets extended to this remote destination. Note This check box does not apply to dual-mode phones that are running SIP, such as DoCoMo N902iL and DoCoMo N906i, nor to dual-mode phones that are running SCCP, such as Nokia S60.</td>
</tr>
<tr>
<td>Enable Mobile Connect</td>
<td>Check the check box to allow an incoming call to ring your desk phone and remote destination at the same time.</td>
</tr>
</tbody>
</table>
When Mobile Connect Is Enabled

**Ring Schedule**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the time</td>
<td>If the Enable Mobile Connect check box is checked for this remote destination, clicking this radio button allows this remote destination to ring all the time. This setting works in conjunction with the setting in the When receiving a call during the above ring schedule pane below.</td>
</tr>
<tr>
<td>As specified below</td>
<td>If the Enable Mobile Connect check box is checked for this remote destination, clicking this radio button allows this remote destination to ring according to the schedule that the subsequent rows specify. This setting works in conjunction with the setting in the When receiving a call during the above ring schedule pane below.</td>
</tr>
<tr>
<td>(day of week)</td>
<td>If the Enable Mobile Connect check box is checked and the As specified below radio button is selected, click the check box for each day of the week when the remote destination should receive calls. You can specify a ring schedule for each day of the week. (day of the week)—Check the check box for a day of the week, such as Monday, to specify the ring schedule for that day. All Day—Click this check box next to a day of the week to specify that the remote destination should ring at all hours of the day as specified by the setting in the When receiving a call during the above ring schedule pane below. (drop-down list box) to (drop-down list box)—For a particular day of the week, specify a ring schedule by choosing a starting time and ending time for that day. Specify the starting time by choosing a value in the drop-down list box that precedes to and specify the ending time by choosing a value in the drop-down list box that follows to. For a particular day, the default ring schedule specifies No Office Hours. The values that you specify in the drop-down list boxes relate to the time zone that you specify in the Time Zone field for the remote destination or mobile identity.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>From the drop-down list box, choose a time zone to use for this remote destination or mobile identity.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The time-of-day access feature uses the time zone that you choose for this remote destination or mobile identity to allow or to block calls to this remote destination or mobile identity.</td>
</tr>
</tbody>
</table>

When receiving a call during the above ring schedule

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always ring this destination</td>
<td>Click this radio button to cause incoming calls to always ring this remote destination according to the Ring Schedule that you specify. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination.</td>
</tr>
</tbody>
</table>
Table 14-7  Remote Destination Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring this destination only if caller is in</td>
<td>Click this radio button to allow incoming calls to ring this remote destination only if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination. From the drop-down list box, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the Call Routing &gt; Class of Control &gt; Access List menu option.) Choosing an access list that contains no members equates to choosing to never ring this destination.</td>
</tr>
<tr>
<td>Do not ring this destination if caller is in</td>
<td>Click this radio button to prevent incoming calls from ringing this remote destination if the caller belongs to the access list that is specified in the drop-down list box and according to the Ring Schedule that you specify in the Ring Schedule pane. This setting applies only if the Enable Mobile Connect check box is checked for this remote destination. From the drop-down list box, choose an access list that applies to this setting. If you want to view the details of an access list, click the View Details link. (To modify an access list, you must use the Call Routing &gt; Class of Control &gt; Access List menu option.) Choosing an access list that contains no members equates to choosing the Always ring this destination radio button.</td>
</tr>
</tbody>
</table>

Association Information

<table>
<thead>
<tr>
<th>Line</th>
<th>This entry displays a line that can associate with this remote destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Association</td>
<td>Check this check box if you want to associate a particular line with this remote destination. You must check a line association check box for Mobile Connect to work for this remote destination.</td>
</tr>
</tbody>
</table>

| Note                                       | Be aware that the line association check box of a line must be checked for Mobile Connect calls to ring this remote destination when a call comes into the directory number that is assigned to that line. |

Additional Information

See the “Related Topics” section on page 14-62.

Mobile Voice Access Directory Number Configuration

Use the Mobile Voice Access window under Media Resources to assign sets of localized user prompts for Mobile Voice Access.

This configuration is required for making calls with the Mobile Voice Access feature. After the gateway collects the required digits from the user to make a call, the call gets transferred to the DN that is configured in this window. This DN can be an internal DN to Cisco Unified Communications Manager and the end user does not need to know the DN. The administrator must configure a dial-peer so that the MVA service can transfer the call from the gateway to this DN. This DN should be also be placed in a
partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN, as configured in the Inbound Calling Search Space for Remote Destination service parameter in the Clusterwide Parameters (System - Mobility) pane.

To assign localized users prompts for Mobile Voice Access, perform the following procedure:

**Procedure**

**Step 1** In the menu bar, choose **Media Resources > Mobile Voice Access**.

**Step 2** Enter values for the parameters that are described in Table 14-8.

**Step 3** Click **Save**.

**Additional Information**

See the “Related Topics” section on page 14-62.

**Mobile Voice Access Configuration Settings**

Table 14-8 describes the available settings in the Mobile Voice Access window. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Voice Access Information</strong></td>
<td></td>
</tr>
<tr>
<td>Mobile Voice Access Directory Number</td>
<td>Enter the internal DN to receive Mobile Voice Access calls from the gateway. Enter a value between 1 and 24 digits in length. You may use the following characters: 0 to 9.</td>
</tr>
<tr>
<td>Mobile Voice Access Partition</td>
<td>From the drop-down list box, choose a partition for Mobile Voice Access. The combination of directory number and partition makes the Mobile Voice Access directory number unique.</td>
</tr>
<tr>
<td><strong>Mobile Voice Access Localization</strong></td>
<td></td>
</tr>
<tr>
<td>Available Locales</td>
<td>This pane displays the locales that have been configured. See the Cisco Unified Communications Manager Locale Installer documentation for details. Use the Down Arrow key to move the locales that you select to the Selected Locales pane.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Cisco Unified Mobility supports a maximum of nine locales. If more than nine locales are installed for Cisco Unified Communications Manager, they will display in the Available Locales pane, but you can only save up to nine locales in the Selected Locales pane. If you attempt to configure more than nine locales for Cisco Unified Mobility, the following message displays: “Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed.”</td>
</tr>
</tbody>
</table>

Table 14-8 Mobile Voice Access Configuration Settings
Gateway Configuration for Enterprise Feature Access

To configure H.323 or SIP gateways for Enterprise Feature Access, two options are available:
- Configuring an H.323 or SIP Gateway for System Remote Access, page 14-50

Additional Information
See the “Related Topics” section on page 14-62.

Configuring an H.323 or SIP Gateway for System Remote Access

If you already have an H.323 or SIP gateway that is configured in Cisco Unified Communications Manager, you can use it to support system remote access. If you do not have an H.323 or SIP gateway, you must add and configure one. For more information, see the “Adding a Cisco IOS H.323 Gateway” section in the Cisco Unified Communications Manager Administration Guide.

Note
When a Mobile Connect call is placed from an internal extension, the system presents only the internal extension as the caller ID. If an H.323 or SIP gateway is used, you can use translation patterns to address this issue.
To configure the gateway, follow these steps.

Procedure

Step 1 Configure the T1/E1 controller for PRI from PSTN.
Sample configuration:
- controller T1 1/0
- framing esf
- linecode b8zs
- pri-group timeslots 1-24

Step 2 Configure the serial interface for the PRI (T1/E1).
Sample configuration:
- interface Serial 1/0:23
- ip address none
- logging event link-status none
- isdn switch-type primary 4ess
- isdn incoming-voice voice
- isdn bchan-number-order ascending
- no cdp enable

Step 3 Load the VXML application from the Cisco Unified Communications Manager server (Publisher).
Sample configuration for IOS Version 12.3 (13) and later:
- application service CCM
  - http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
Sample configuration before IOS Version 12.3(12):
- call application voice Unified CCM
  - http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml

Note Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

Step 4 Configure the dial-peer to associate Mobile Connect application with system remote access.
Sample configuration for IOS 12.3(13) and later:
- dial-peer voice 58888 pots
- service CCM (Mobile Connect VXML application)
- incoming called-number 58888
Sample configuration for IOS 12.3(12) and earlier:
- dial-peer voice 100 pots
- application CCM (Mobile Connect VXML application)
incoming called-number 58888 *(where 58888 represents the Mobile Voice Access number)*

**Step 5** Add a dial-peer to transfer the calls to the Mobile Voice Access DN that is configured in the “Mobile Voice Access Directory Number Configuration” section on page 14-48.

Sample configuration for primary Cisco Unified Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

**Note** This specifies the Mobile Voice Access DN that is configured with the Media Resources > Mobile Voice Access menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Unified Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

**Note** This specifies the Mobile Voice Access DN that is configured with the Media Resources > Mobile Voice Access menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for SIP gateway voip dial-peer:

- dial-peer voice 80 voip
- destination-pattern <Mobile Voice Access DN>
- rtp payload-type nse 99
- session protocol sipv2
- session target ipv4:10.194.107.80
- incoming called-number .T
Additional Information
See the “Related Topics” section on page 14-62.

Configuring an H.323 Gateway for System Remote Access by Using Hairpinning

If you do not have an H.323 gateway but want to use a H.323 gateway only to support System Remote Access, you must add and configure the gateway. For more information, see the “Adding a Cisco IOS H.323 Gateway” section in the Cisco Unified Communications Manager Administration Guide.

To configure the gateway, follow these steps.

Procedure

**Step 1**
Load the VXML application from the Cisco Unified Communications Manager server (Publisher).

Sample configuration for IOS Version 12.3(13) and later:
- application service CCM
- `http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml`

Sample configuration before IOS Version 12.3(12):
- call application voice Unified CCM
- `http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml`

**Note**
Although VXML was added in Version 12.2(11), Versions 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues, and you should not use them.

**Step 2**
Configure the dial-peer to associate Mobile Connect application with system remote access.

Sample configuration for IOS 12.3(13) and later:
- dial-peer voice 1234567 voip
- service CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip_address of call manager>

Sample configuration for IOS 12.3(12) and earlier:
- dial-peer voice 1234567 voip
- application CCM
- incoming called-number 1234567
- codec g711u
- session target ipv4:<ip_address of call manager>
Step 3 Add a dial-peer for transferring calls to the Mobile Voice Access DN that is configured in the “Mobile Voice Access Directory Number Configuration” section on page 14-48.

Sample configuration for primary Cisco Communications Manager:

- dial-peer voice 101 voip
- preference 1
- destination-pattern <Mobile Voice Access DN>

**Note** This specifies the Mobile Voice Access DN that is configured with the Media Resources > Mobile Voice Access menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.3
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Sample configuration for secondary Cisco Communications Manager (if needed):

- dial-peer voice 102 voip
- preference 2
- destination-pattern <Mobile Voice Access DN>

**Note** This specifies the Mobile Voice Access DN that is configured with the Media Resources > Mobile Voice Access menu option. If a generic dial-peer is already configured to terminate the calls and is consistent with the Mobile Voice Access DN, you do not need to perform this step.

- session target ipv4:10.1.30.4
- voice-class h323 1
- codec g711ulaw
- dtmf-relay h245-alphanumeric
- no vad

Step 4 Configure hairpin.

- voice service voip
- allow-connections h323 to h323

Step 5 On the Cisco Unified Communications Manager, create a new route pattern to redirect the incoming MVA number to the H.323 gateway that has the vxml script loaded. Ensure that the Incoming CSS of the gateway can access the partition in which the new route pattern gets created.

Additional Information

See the “Related Topics” section on page 14-62.
Enterprise Feature Access Two-Stage Dialing

To configure enterprise feature access two-stage dialing, use the following procedure.

**Procedure**

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

**Step 2** For the Cisco CallManager service, set the following service parameters in the Clusterwide Parameters (System - Mobility) area:

- Set the Enable Enterprise Feature Access service parameter to **True**.
- Set the Matching Caller ID for Remote Destination service parameter. Choose either **Complete Match** or **Partial Match**. If you choose Partial Match, proceed to set a value for the Number of Digits for Caller ID Partial Match service parameter.
- If you set the Matching Caller ID for Remote Destination service parameter to **Partial Match**, set the Number of Digits for Caller ID Partial Match service parameter.

**Step 3** To save the service parameter settings, click **Save**.

**Step 4** Choose **Call Routing > Mobility > Enterprise Feature Access Configuration**.

**Step 5** In the Mobility Enterprise Feature Access Configuration window, configure the Enterprise Feature Access DID by specifying a value in the (Access Number Information) Number field. (This field specifies the same DID that is called to invoke midcall features like Transfer and Conference.)

**Step 6** Specify the partition by choosing a value for the Route Partition.

**Step 7** To save the Mobility Enterprise Feature Access Configuration settings, click **Save**.

**Step 8** Ensure that the outbound VOIP dial-peer that is used on the gateway for the initial call leg over to the remote destination (mobile phone) has DTMF-relay configuration in it, so the DTMF codes can get passed through to Cisco Unified Communications Manager.

**Step 9** Configure dial-peers on the gateway that receives the second-stage inbound call to the Enterprise Feature Access DID, so the call gets forwarded to the Cisco Unified Communications Manager. Ensure that the VOIP dial-peer has the DTMF-relay configuration in it.

**Note**

If a generic dial-peer is already configured to forward the calls to Cisco Unified Communications Manager and is consistent with the EFA DN, you do not need to perform this step. Ensure that the VOIP dial-peer for this call leg also has a configured DTMF-relay command.

See the *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager* for the list of steps that you need to configure Enterprise Feature Access.

When a caller calls the Enterprise Feature Access DID, Cisco Unified Communications Manager matches the calling number to the destination number that is configured in the Remote Destination Configuration window. In the scenario where Cisco Unified Communications Manager Administration
inserts the digit 9 to get an outside line, the administrator can manipulate the quantity of digits of this number by modifying these service parameters in the Clusterwide Parameters (System - Mobility) section:

- Matching Caller ID with Remote Destination
- Number of Digits for Caller ID Partial Match

No IVR exists with this configuration, so callers do not receive a prompt.

See the User Guide of the remote phone model for the steps that users perform to make outbound calls and to use Mobile Voice Access. Keep in mind that, when you use Enterprise Feature Access, each entry must end with the # (octothorpe) character.

**Note**

When calling the Mobile Voice Access DN or Enterprise Feature Access DN, the gateway device must present the exact number of digits that are configured as the Mobile Voice Access DN or Enterprise Feature Access DN. Translation patterns or other called number modification cannot be used to match the MVA or EFA numbers either by stripping digits or by adding digits to the number that the gateway presents. Because Cisco Unified Mobility intercepts the call at the gateway layer, the feature behaves thus by design.

**Note**

Unlike Mobile Voice Access (MVA), Enterprise Feature Access (EFA) identifies the user based solely on caller ID. If the system receives no inbound caller ID or receives a value that does not match a remote destination, the EFA call fails. With MVA, if the caller ID does not match, the user gets prompted to enter the user remote destination number. EFA does not provide this capability because no IVR prompts exist. In both cases, after the user is identified, the user authenticates by using the same PIN number.

**Additional Information**

See the “Related Topics” section on page 14-62.

**Mobility Enterprise Feature Configuration**

To configure mobility enterprise feature configuration, see the following section:

- Mobility Enterprise Feature Configuration Settings, page 14-56

**Additional Information**

See the “Related Topics” section on page 14-62.

**Mobility Enterprise Feature Configuration Settings**

In Cisco Unified Communications Manager Administration, use the Call Routing > Mobility > Enterprise Feature Access Configuration menu path to configure mobility enterprise feature configuration.

The Mobility Enterprise Feature Configuration window allows you to configure mobility enterprise feature access (EFA) numbers. These numbers can then associate with mobility profile(s) for use.
Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-9 describes the available settings in the Mobility Enterprise Feature Configuration window. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

Table 14-9 Mobility Enterprise Feature Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Number Information</td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td>Enter the DID number that is required for enterprise feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones.</td>
</tr>
<tr>
<td></td>
<td>Note: Ensure that each DID number is unique.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>From the drop-down list box, choose the partition of the DID that is required for enterprise feature access.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the Mobility Enterprise Feature Access number.</td>
</tr>
<tr>
<td>Default Enterprise Feature Access Number</td>
<td>Check this box to make this Enterprise Feature Access number the default for this system.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 14-62.

Handoff Mobility Configuration

To configure handoff mobility configuration, see the following section:

- Handoff Mobility Configuration Settings, page 14-57

Additional Information

See the “Related Topics” section on page 14-62.

Handoff Mobility Configuration Settings

In Cisco Unified Communications Manager Administration, use the Call Routing > Mobility > Handoff Configuration menu path to configure handoff mobility configuration.

The Handoff Mobility Configuration window allows you to configure a handoff number and/or partition for dual-mode phones between the Wi-Fi and Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA) networks.
Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Table 14-10 describes the available settings in the Handoff Mobility Configuration window. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handoff Configuration Information</td>
<td></td>
</tr>
<tr>
<td>Handoff Number</td>
<td>Enter the DID number for handoff between the Wi-Fi and GSM or CDMA networks. The handoff feature requires this number. For numbers that start with the international escape character +, you must precede the + with a backslash (). Example: +15551234.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>From the drop-down list box, choose the partition to which the handoff direct inward dial (DID) number belongs.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 14-62.

Mobility Profile Configuration

To configure mobility profiles, see the following section:

- Mobility Profile Configuration Settings, page 14-58

Additional Information

See the “Related Topics” section on page 14-62.

Mobility Profile Configuration Settings

In Cisco Unified Communications Manager Administration, use the Call Routing > Mobility > Mobility Profile menu path to configure mobility profiles.

Mobility profiles specify profiles where you can configure Dial-via-Office Forward or Dial-via-Office Reverse settings for a mobile client. After you configure a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location. You specify either DVO-F or DVO-R for a particular mobility profile, but you configure both the DVO-F and DVO-R settings for the mobility profile.

Mobility profiles can associate with a standalone Cisco Unified Mobile Communicator mobile identity or with a Cisco Unified Mobile Communicator-enabled dual-mode mobile identity. Standard, single-mode remote destinations cannot associate with a mobility profile.

Mobility profiles settings can be changed only by administrators; users cannot change the settings in a mobility profile.
Tips About Configuring Mobility Profiles

Before you start to configure mobility profiles, consider the design issues that follow.

If a client associates with a mobility profile and a DVO-R call is configured, the caller ID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-R caller ID from the mobility profile (if this value is configured in the mobility profile)
2. EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default EFA DN

The administrator must configure the caller ID value in at least one of the preceding settings for the DVO-R call to succeed.

If a client associates with a mobility profile and a DVO-F call is configured, the DID value in the 183 SIP message gets retrieved according to the following preference order:

1. DVO-F service access number from mobility profile (if this value is configured in the mobility profile)
2. DVO-F EFA DN from mobility profile (if this value is configured in the mobility profile)
3. Default service access number, which is configured in the Service Parameter Configuration window
4. Default EFA DN

For a DVO-F call, the client needs to make an incoming call to Cisco Unified Communications Manager that terminates at a particular DID. The administrator must configure this DID in at least one of the preceding settings for the DVO-F call to succeed.

Cisco Unified Communications Manager identifies an incoming PSTN call (made by the client) as DVO-F by matching the called number (that is, the DID number that was sent in the 183 SIP message) in the following priority order:

If a mobility profile associates with the client

1. DVO-F EFT DN from mobility profile (if this value is configured)
2. DVO-F service access number from mobility profile (if this value is configured)

If no mobility profile associates with the client:

1. Default EFA DN
2. Default service access number

Also consider the following requirements when you configure mobility profiles:

- Administrator should configure the PSTN gateway so that matching of the called party can take place.
- EFA DN and service access number always comprise a pair: both of these values get retrieved from the mobility profile and must match in the mobility profile, or both default values get retrieved and the default values must match.
Using the GUI
For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table
Table 14-11 describes the available settings in the Mobility Profile Configuration window. For more information on Cisco Unified Mobility, see the “Related Topics” section on page 14-62.

Table 14-11 Mobility Profile Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobility Profile Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for this mobility profile, up to 50 characters in length. Valid values specify upper- and lowercase letters, numeric digits (0 through 9), periods (.), dashes (-), underscores (_) and spaces ( ).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this mobility profile.</td>
</tr>
<tr>
<td>Mobile Client Calling Option</td>
<td>From the drop-down list box, choose a mobile client calling option:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial via Office Reverse</strong>—Choose this option for the mobile client to make Dial-via-Office Reverse calls.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial via Office Forward</strong>—Choose this option for the mobile client to make Dial-via-Office Forward calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The administrator configures either DVO-R or DVO-F for automatic selection by the client for any DVO calls that the user makes. Users can make the opposite type of DVO call than what the administrator has configured by explicitly choosing their DVO call type on their mobile devices.</td>
</tr>
<tr>
<td><strong>Dial-via-Office Forward Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Service Access Number</td>
<td>Enter the DID number that is required for Dial-via-Office Forward feature access. This number supports transfer, conference, resume, and two-stage dialing from smartphones. This number gets returned in the 183 SIP message that Cisco Unified Communications Manager sends to the client. The client uses this value as a dial-in DID. Cisco Unified Communications Manager uses this value as the first preference to search when completing a DVO-F call. If this value is not configured, Cisco Unified Communications Manager uses the value in the Enterprise Feature Access Number/Partition field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Ensure that each DID number is unique.</td>
</tr>
</tbody>
</table>
Mobility Softkey Configuration

To configure a Mobility softkey for the phone user that uses Mobile Connect, perform the following procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Device &gt; Device Settings &gt; Softkey Template.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>To list the existing templates, click Find.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>To create the new template, click Standard User and then click Copy.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter a name and description for the Softkey template and click Save.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Select Configure Softkey Layout from the Go next to Related Link menu in the upper, right corner of the window and click Go.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Select On Hook from the pull-down list box.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Add Mobility to the selected Softkeys and click Save.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Select Connected from the pull-down list box.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Add Mobility to the selected Softkeys and click Save.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Open the Phone Configuration window and associate the Softkey Template with the created Softkey template. See “Configuring Cisco Unified IP Phones” in the Cisco Unified Communications Manager Administration Guide.</td>
</tr>
</tbody>
</table>
**Step 11** Choose the Owner User ID for the Mobile Connect phone user.

**Step 12** Click **Save**.

---

**Additional Information**

See the “Related Topics” section on page 14-62.

---

**Related Topics**

- Configuration Checklist for Cisco Unified Mobility, page 14-2
- Introducing Cisco Unified Mobility, page 14-4
- Definitions, page 14-5
- List of Cisco Unified Mobility Features, page 14-6
- Other Benefits of Cisco Unified Mobility Features, page 14-7
- Mobile Connect, page 14-8
- Mobile Voice Access, page 14-11
- Time-of-Day Access, page 14-12
- Time-of-Day Access Configuration, page 14-13
- Important Notes for Time-of-Day Access, page 14-14
- Directed Call Park via DTMF, page 14-15
- SIP URI Dialing, page 14-16
- Intelligent Session Control, page 14-17
- Interactions and Limitations, page 14-27
- Licensing, page 14-29
- Number of Supported Calls, page 14-30
- Auto Call Pickup, page 14-28
- System Requirements, page 14-34
- Migrating from Cisco Unified MobilityManager, page 14-35
- Configuring Cisco Unified Mobility, page 14-35
- Configuration Checklist for Cisco Unified Mobility, page 14-2
- Access List Configuration, page 14-36
- Remote Destination Profile Configuration, page 14-39
- Remote Destination Configuration, page 14-43
- Mobile Voice Access Directory Number Configuration, page 14-48
- Gateway Configuration for Enterprise Feature Access, page 14-50
- Enterprise Feature Access Two-Stage Dialing, page 14-55
- Mobility Enterprise Feature Configuration, page 14-56
- Handoff Mobility Configuration, page 14-57
Chapter 14  Cisco Unified Mobility

- Mobility Profile Configuration, page 14-58
- Mobility Softkey Configuration, page 14-61
- End User Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Licenses for Cisco Unified Mobility, Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration, page 15-1

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Security Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
- Applicable Cisco Unified IP Phone User Guides
- Applicable Cisco Unified IP Phone Administration Guides
- “Cisco Mobility Applications” chapter in Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager
- “Configuring Cisco Unified Communications Manager for Use With Cisco Unified Mobility Advantage” chapter in the Installation and Administration Guide for Cisco Unified Mobility Advantage
Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration

Cisco Unified Communications Manager provides certain functionality for Cisco Unified Mobile Communicator clients in conjunction with a Cisco Unified Mobility Advantage server. This chapter discusses the features and the required configurations on both servers.

Cisco Unified Communications Manager provides the following functionality to Cisco Unified Mobile Communicator users:

- Dial-via-Office Reverse Callback
- Dial-via-Office Forward
- Call log monitoring, which allows users to review their office call history from their mobile devices
- Mobile Connect and the ability to enable and disable Mobile Connect from the mobile device
- Ability to transfer active Dial-via-Office calls between the mobile device and the desktop phone

For further configuration details about configuring the Cisco Unified Mobility Advantage server and the Cisco Unified Mobile Communicator client, see the following documentation:

- “Configuring a Cisco Unified Mobility Advantage Server Security Profile” chapter in the Cisco Unified Communications Manager Security Guide

See the user guide for a particular Cisco Unified IP Phone for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified CM User Options windows.

Note

For details of configuring Cisco Unified Mobility features that you configure within Cisco Unified Communications Manager and that do not require configuration of Cisco Unified Mobile Communicator nor Cisco Unified Mobility Advantage, see the “Cisco Unified Mobility” chapter.
This chapter includes information on the following topics:

- **Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage**, page 15-2
- **Introducing Cisco Unified Mobility with Cisco Unified Mobility Advantage**, page 15-4
  - Definitions, page 15-5
  - List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage, page 15-5
  - Cisco Unified Mobile Communicator, page 15-7
  - Dial-via-Office Reverse Callback, page 15-10
  - Dial-via-Office Forward, page 15-11
  - Session Resumption, page 15-14
  - Use Case Scenarios for Cisco Unified Mobility Features, page 15-15
- **Interactions and Limitations**, page 15-18
  - Limitations, page 15-18
- **System Requirements**, page 15-19
- **Configuring Cisco Unified Mobility with Cisco Unified Mobility Advantage**, page 15-19
- **Related Topics**, page 15-20

### Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage

Configure the Cisco Unified Mobility Advantage server to communicate with Cisco Unified Communications Manager. See the following documentation for configuration information:


For more information on Cisco Unified Mobility features that are available upon configuration of the Cisco Unified Mobility Advantage server, see the “List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage” section on page 15-5.

For more information on Cisco Unified Mobility features that are native to Cisco Unified Communications Manager and that do not require configuration of Cisco Unified Mobile Communicator nor Cisco Unified Mobility Advantage, see the “List of Cisco Unified Mobility Features” section on page 14-6 in the “Cisco Unified Mobility” chapter.
Table 15-1 summarizes the procedures for configuring Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage to operate with Cisco Unified Communications Manager. For detailed instructions, see the chapters and sections that the table references. In addition, see the “Related Topics” section on page 15-20.

### Table 15-1  
Cisco Unified Mobility with Cisco Unified Mobility Advantage Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| **Step 1**          | **Installing and Configuring Cisco Unified Mobility Advantage, Release 7.1, at**  
**Configuration guides for Cisco Unified Mobility Advantage, Release 7.1, at**  
**End User Configuration, Cisco Unified Communications Manager Administration Guide** |
| On the Cisco Unified Mobility Advantage server, configure a Cisco Unified Communications Manager adapter that points to up to two nodes within the Cisco Unified Communications Manager cluster.  
Within Cisco Unified Mobility Advantage, specify a SOAP-enabled application user name and password on the adapter.  
Set the Communications Manager setting on the adapter configuration window to 8.x.  
You can also configure a security context or profile on the adapter to provide a secure connection to Cisco Unified Communications Manager, if desired. |  
**Installing and Configuring Cisco Unified Mobility Advantage, Release 7.1, at**  
**Configuration guides for Cisco Unified Mobility Advantage, Release 7.1, at**  
**End User Configuration, Cisco Unified Communications Manager Administration Guide** |
| **Step 2**          |  
Activate and provision the user for the Cisco Unified Mobile Communicator client on the Cisco Unified Mobility Advantage server. The user ID on the Cisco Unified Mobility Advantage server must match the user ID and end-user account within Cisco Unified Communications Manager. |  
**Installing and Configuring Cisco Unified Mobility Advantage, Release 7.1, at**  
**Configuration guides for Cisco Unified Mobility Advantage, Release 7.1, at**  
**End User Configuration, Cisco Unified Communications Manager Administration Guide** |
| **Step 3**          |  
Upon activation, the user or Cisco Unified Mobility Advantage administrator should provision the user mobile phone for Cisco Unified Mobile Communicator on the Cisco Unified Mobility Advantage server and enter the mobile phone number.  
Configure this number to match the Mobility Identity directory number that is configured within Cisco Unified Communications Manager exactly. |  
**Installing and Configuring Cisco Unified Mobility Advantage, Release 7.1, at**  
**Configuration guides for Cisco Unified Mobility Advantage, Release 7.1, at**  
**Remote Destination Configuration Settings, page 14-44** |
Introducing Cisco Unified Mobility with Cisco Unified Mobility Advantage

Administrators configure the basic setup of Cisco Unified Mobility for end users by using the Cisco Unified Communications Manager Administration windows. See the “Cisco Unified Mobility” chapter for details.

Be aware that special configuration in Cisco Unified Communications Manager Administration is required for features that the Cisco Unified Mobile Communicator provides on user phones in conjunction with the Cisco Unified Mobility Advantage server.

This section discusses the following topics:

- Definitions, page 15-5
- List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage, page 15-5
- Cisco Unified Mobile Communicator, page 15-7
- Dial-via-Office Reverse Callback, page 15-10
- Dial-via-Office Forward, page 15-11
- Session Resumption, page 15-14
- Use Case Scenarios for Cisco Unified Mobility Features, page 15-15

Additional Information

See the “Related Topics” section on page 15-20.
Definitions

Table 15-2 provides definitions of terms that are related to Cisco Unified Mobility with Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Mobility Advantage</td>
<td>Cisco Unified Mobility Advantage specifies server software that is deployed behind the enterprise firewall to connect employee mobile phones to company resources. Cisco Unified Mobility Advantage runs in conjunction with the Cisco Unified Mobile Communicator client, which runs on employee mobile devices.</td>
</tr>
<tr>
<td>Cisco Unified Mobile Communicator</td>
<td>Cisco Unified Mobile Communicator specifies the client software that runs on supported mobile phones. Cisco Unified Mobile Communicator runs in conjunction with a Cisco Unified Mobility Advantage server to provide access to enterprise services.</td>
</tr>
<tr>
<td>Cisco Mobile 7.x</td>
<td>Cisco Unified Mobile Communicator clients that connect to Cisco Unified Communications Manager through a Cisco Unified Mobility Advantage proxy server.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 15-20.

List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage

This section provides a list of Cisco Unified Mobility features that are available to mobile phone users when the required configuration for Cisco Unified Mobility Advantage has also been performed. This material discusses configuration within Cisco Unified Communications Manager Administration.

For a complete discussion of Cisco Unified Mobility Advantage configuration, see the following documentation:


The following entities and features require configuration of Cisco Unified Mobility in Cisco Unified Communications Manager Administration as well as configuration of Cisco Unified Mobility Advantage:

- Cisco Unified Mobile Communicator—Cisco Unified Mobile Communicator specifies a phone device that is running the Cisco Unified Mobile Communicator client and communicates via a data channel back to the Cisco Unified Mobility Advantage server by using Mobility Multiplexing Protocol (MMP). You configure the Cisco Unified Mobile Communicator in the Phone Configuration window in Cisco Unified Communications Manager Administration. See the “Cisco Unified Mobile Communicator” section on page 15-7 for a detailed discussion.
Chapter 15  Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration

Introducing Cisco Unified Mobility with Cisco Unified Mobility Advantage

- **Dial-via-Office Reverse Callback**—The Dial-via-Office Reverse Callback feature resembles the Mobile Voice Access feature, except that Cisco Unified Communications Manager makes both calls. From the Cisco Unified Mobile Communicator client, using the data channel, the phone initiates the Dial-via-Office Reverse Callback feature. Cisco Unified Communications Manager then calls the mobility identity first. When the mobility identity answers, Cisco Unified Communications Manager calls the destination number. See the “Dial-via-Office Reverse Callback” section on page 15-10 for a detailed discussion.

- **Dial-via-Office Forward**—The Dial-via-Office Forward feature resembles Mobile Voice Access, except that the request comes through data channel instead of from IVR. From the Cisco Unified Mobile Communicator (CUMC) client, using the data channel, the phone initiates the Dial-via-Office Forward feature. Cisco Unified Communications Manager then returns the Enterprise Feature Access (EFA) Number through the data channel. The mobility identity (MI) calls the Enterprise Feature Access number, and Cisco Unified Communications Manager calls the destination number. See the “Dial-via-Office Forward” section on page 15-11 for a detailed discussion.

- **Session Resumption**—This feature provides one-touch reconnect to the last dialed target in case of any unexpected DVO-F call drop. This feature helps users who are making DVO-F calls and who experience a network failure. Prior to the implementation of this feature, if the mobile user pressed Redial (either by calling the last dialed number from the phone call history or by pressing Call Back if the phone provides such an option), the redial number specified the Dial-via-Office Forward Feature Access Number (configured under Service Parameter) or Enterprise Feature Access Number (configured under Call Routing > Mobility > Enterprise Feature Access Number Configuration). Cisco Unified Communications Manager treated the call as an Enterprise Feature Access call, and the user could not connect to the last redial target. With the implementation of this feature, when the user presses Redial, Cisco Unified Communications Manager reconnects the mobile user with the actual target DN. See the “Session Resumption” section on page 15-14 for a detailed discussion.

The following features, which were originally part of Cisco Unified Mobility Manager, now reside in Cisco Unified Communications Manager:

- **Mobile Connect**—See the “Cisco Unified Mobility” chapter for details.
- **Desktop Call Pickup**—See the “Cisco Unified Mobility” chapter for details.
- **Mobile Voice Access**—See the “Cisco Unified Mobility” chapter for details.
- **Access List**—See the “Cisco Unified Mobility” chapter for details.

Cisco Unified Communications Manager also supports the following Cisco Unified Mobility features:

- **Midcall Enterprise Feature Support Using DTMF**—See the “Cisco Unified Mobility” chapter for details.
- **Two-stage Dialing**—See the “Cisco Unified Mobility” chapter for details.
- **Dual-mode Phone Support**—See the “Cisco Unified Mobility” chapter for details.
- **Manual Handoff of Calls on a Dual-mode Phone**—See the “Cisco Unified Mobility” chapter for details.
- **Time-of-Day Access**—See the “Cisco Unified Mobility” chapter for details.
- **Directed Call Park via DTMF**—See the “Cisco Unified Mobility” chapter for details.
- **SIP URI Dialing**—See the “Cisco Unified Mobility” chapter for details.
See the “Other Benefits of Cisco Unified Mobility Features” section on page 14-7 for a discussion of other benefits of Cisco Unified Mobility features, such as simultaneous desktop ringing, single enterprise voice mailbox, system remote access, caller ID, remote on/off control, call tracing, security and privacy for Mobile Connect calls, and smartphone support.

Additional Information
See the “Related Topics” section on page 15-20.

Cisco Unified Mobile Communicator

The Cisco Unified Mobile Communicator specifies a device type that you can configure in Cisco Unified Communications Manager Administration in the Phone Configuration window. The Cisco Unified Mobile Communicator uses Mobility Multiplexing Protocol (MMP) to communicate via the mobile phone data connection with the Cisco Unified Mobility Advantage server, which in turn registers the device with Cisco Unified Communications Manager through SIP. The Cisco Unified Mobile Communicator uses one Device License Unit (DLU) if the user has a desktop phone and three DLUs if the user does not have a desktop phone.

See the following topics for configuration details:
- Cisco Unified Mobile Communicator Configuration, page 15-8
- Cisco Unified Mobile Communicator Configuration Details, page 15-9

Additional Information
See the “Related Topics” section on page 15-20.
### Cisco Unified Mobile Communicator Configuration

Table 15-3 summarizes the procedures for configuring the Cisco Unified Mobile Communicator for Cisco Unified Mobility. For detailed instructions, see the information that the table references.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In Cisco Unified Communications Manager Administration, configure a Cisco Unified Mobile Communicator device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Prior to configuring the Cisco Unified Mobile Communicator device within Cisco Unified Communications Manager, make sure the user has been mobility enabled as described in the “Configure user accounts” step of the “Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage” section of the “Cisco Unified Mobility” chapter.</td>
</tr>
<tr>
<td>Use the <strong>Device &gt; Phone</strong> menu option. For Phone Type, choose Cisco Unified Mobile Communicator.</td>
<td>Configuration Checklist for Cisco Unified Mobility, page 14-2</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Make sure that you check the Enable Mobility check box in the End User Configuration window.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Checking the Enable Mobility check box triggers licensing to consume device license units (DLUs) for mobile connect.</td>
</tr>
</tbody>
</table>

**Step 2** | In Cisco Unified Communications Manager Administration, configure a security profile for a Cisco Unified Mobility Advantage server. |
| Use the **System > Security Profile > CUMA Server Security Profile** menu option. | See the Cisco Unified Communications Manager Security Guide for details. |

**Step 3** | In Cisco Unified Communications Manager Administration, configure the enterprise feature access directory number (DN). |
| Use the **Call Routing > Mobility > Enterprise Feature Access Configuration** menu option. | Mobility Enterprise Feature Configuration, page 14-56 |
| **Note** | You must perform this configuration step for the Dial-via-Office features to work. |

**Step 4** | Allow the Cisco Unified Mobility Advantage client to register with Cisco Unified Communications Manager. |
| See the Cisco Unified Communications Manager Security Guide for details. |

**Step 5** | In the Cisco Unified CM User Options windows, configure end-user settings for the Cisco Unified Mobile Communicator, such as the following settings: |
| | • Device—End user specifies his own Cisco Unified Mobile Communicator. |
| | • Remote Destinations—End user chooses his own Cisco Unified Mobile Communicator as the remote destination profile. |
| See the user guide for a particular Cisco Unified IP Phone model. |
Additional Information
See the “Related Topics” section on page 15-20.

Cisco Unified Mobile Communicator Configuration Details

When you configure a Cisco Unified Mobile Communicator, keep in mind the following configuration requirements as you configure the fields in the Phone Configuration window:

- When configuring a new Cisco Unified Mobile Communicator, select the Cisco Unified Mobile Communicator phone type in the Phone Type drop-down list box.
- Device Name—Ensure this name is unique. You need no MAC address.
- Mobility User ID—You must configure this field. You can only choose the user ID of an end user for which the Enable Mobility check box in the Mobility Information pane of the End User Configuration window (User Management > End User) has been checked.
- Mobility Identity—This field must specify the Cisco Unified Mobile Communicator-enabled smartphone mobile number as the destination number. Be aware that the Mobility Identity configuration characteristics are identical to those of the Remote Destination configuration. To access the field, click the Add New Mobility Identity link in the Phone Configuration window, which takes you to the Remote Destination Configuration window so that you can add a mobile identity.
- Rerouting Calling Search Space—Ensure that this field is configured for basic calls to work. This setting applies to the Cisco Unified Mobile Communicator. This setting gets used to route calls to the mobility identity (that is, the Cisco Unified Mobile Communicator client phone). The setting gets used to route the Dial-via-Office callback call leg toward the mobility identity and to route the call leg toward the mobility identity for Mobile Connect/SNR calls.
- Calling Search Space—Ensure that this field is configured for basic calls to work. This setting gets used to route calls from the mobility identity. The setting gets used to route the call leg toward the dialed or target phone for Dial-via-Office calls.
- DND Option—The Cisco Unified Mobile Communicator only supports the Call Reject DND option. Ensure that a directory number is assigned to the Cisco Unified Mobile Communicator.

Keep in mind these other configuration requirements that apply to the Cisco Unified Mobile Communicator:

- Due to the lack of an integrated End User Configuration window for Cisco Unified Communications Manager and the Cisco Unified Mobility Advantage server, the Cisco Unified Mobile Communicator client user must configure identical remote destination numbers in both Cisco Unified Communications Manager Administration and in the Cisco Unified Mobility Advantage server.
- If a Cisco Unified Mobile Communicator client user ever changes his SIM card, the user must update the mobile number in the Cisco Unified Mobility Advantage server by deleting the old mobile phone number and adding the new mobile phone number. The corresponding configuration must take place in Cisco Unified Communications Manager Administration as well.
- Ensure Cisco Unified Communications Manager nodes are statically created in the Cisco Unified Mobility Advantage server administration console.
- The Cisco Unified Mobility Advantage server only uses AXL to update the Cisco Unified Communications Manager database but does not listen to Cisco Unified Communications Manager database change notifications.
General Considerations

Keep in mind the following general considerations for the Cisco Unified Mobile Communicator device:

- You can add one or more remote destinations in addition to the mobility identity to the Cisco Unified Mobile Communicator device (similar to the remote destination profile).
- No automatic migration support exists. You must manually reconfigure the device as a Cisco Unified Mobile Communicator device.
- Only the first call gets supported because, in 2.5G, the data channel does not remain available after the voice call connects.
- The Cisco Unified Mobility Advantage server can activate only one Cisco Unified Mobile Communicator device per user. (A user can have multiple mobile phones configured within Cisco Unified Mobility Advantage, but only one of mobile phones can be actively connected to the Cisco Unified Mobility Advantage server at a given time.)
- In configuration of the Cisco Unified Mobile Communicator device, the reroute CSS and CSS represent key considerations.

Additional Information

See the “Related Topics” section on page 15-20.

Dial-via-Office Reverse Callback

The Dial-via-Office Reverse (DVO-R) Callback feature resembles the Mobile Voice Access feature, except that Cisco Unified Communications Manager makes both calls. From the Cisco Unified Mobile Communicator client, using the data channel, the phone initiates the Dial-via-Office Reverse Callback feature by sending a SIP INVITE message to Cisco Unified Communications Manager. Cisco Unified Communications Manager then calls the mobility identity (Cisco Unified Mobile Communicator client) first. When the mobility identity answers, Cisco Unified Communications Manager calls the dialed (target) number.

In all Dial-via-Office scenarios, the callback leg from Cisco Unified Communications Manager either to the Cisco Unified Mobile Communicator client mobile phone/mobility identity or to an alternate number always specifies the caller ID of the Enterprise Feature Access DID. The caller ID that gets sent for the call leg from Cisco Unified Communications Manager to the target or dialed number always specifies the user enterprise desk number (based on the shared line between the user desktop phone and the Cisco Unified Mobile Communicator client device type that is configured within Cisco Unified Communications Manager).

Example of Dial-via-Office Reverse Callback

The following example illustrates the sequence of events that takes place in an instance of dial-via-office reverse callback:

- Phone sends INVITE 2000 with the callback number that is specified in the SDP parameter “c=PSTN E164 4085551234.”
- Cisco Unified Communications Manager sends back 183 Session In Progress with Enterprise Feature Access Number DID (4085556666) in SDP parameter.
- Cisco Unified Communications Manager calls back mobility identity 4085551234.
- When the mobility identity answers the call, Cisco Unified Communications Manager redirects the call to the target DN 2000.
Use Case Scenarios
See the “Use Case Scenarios for Dial-via-Office Reverse Callback” section on page 15-16 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Limitations for Dial-via-Office Reverse Callback Feature
See the “Dial-via-Office Limitations (DVO-R and DVO-F)” section on page 15-18 for a list of limitations that apply to this feature.

Additional Information
See the “Related Topics” section on page 15-20.

Dial-via-Office Forward

Users that have Cisco Mobile, a Cisco Unified Mobile Communicator application, installed on their mobile devices can take advantage of the Dial-via-Office Forward feature. Cisco Unified Mobile Communicator invokes the Dial-via-Office Forward feature from the mobile device through SIP signaling over the data channel between Cisco Unified Mobile Communicator-Cisco Unified Mobility Advantage and Cisco Unified Mobility Advantage-Cisco Unified Communications Manager to initiate calls to a final target. Because the calls are anchored at the enterprise, the feature offers a cost-saving solution to Cisco Unified Mobile Communicator mobile users.

Only Cisco Unified Mobile Communicator devices with the Cisco Mobile client can invoke the Dial-via-Office Forward feature.

Cisco Unified Communications Manager returns the Dial-via-Office Forward (DVO-F) service access number, if the DVO-F service access number has been configured, or the Enterprise Feature Access (EFA) directory number (DN) through the data channel. The Cisco Unified Mobile Communicator client that runs on the mobile phone calls the number that it receives from Cisco Unified Communications Manager. The phone number of the mobile device that makes the DVO-F call gets matched against configured Mobility Identities (MI), thus ensuring that the system places only those calls that authorized users make. If a match occurs, the call request gets sent to the target party. Both complete match and partial match get supported, depending on the setting of the Matching Caller ID with Remote Destination service parameter.

This section covers the following topics for the Dial-via-Office Forward feature:

- Configuration of Dial-via-Office Forward in Cisco Unified Communications Manager Administration, page 15-12
- Dial-via-Office Forward Service Access Number, page 15-12
- Globalization Support for EFA DN and DVO-F Service Access Number, page 15-13
- Use Case Scenarios for Dial-via-Office Forward, page 15-13
- Dial-via-Office Forward Call Characteristics, page 15-13
- Example of Dial-via-Office Forward, page 15-13
- Dial-via-Office Forward Configuration Tips, page 15-14
- Limitations for Session Resumption Feature, page 15-15
Configuration of Dial-via-Office Forward in Cisco Unified Communications Manager Administration

The following configuration must take place in Cisco Unified Communications Manager Administration for the Dial-via-Office Forward feature to be enabled:

- **Call Routing > Mobility Configuration**
  The value of the Enterprise Feature Access Directory Number setting should match the called number and should belong to the correct partition.

- **System > Service Parameters**
  The Dial-via-Office Service Access Number can specify an alternate number.

**Dial-via-Office Forward Service Access Number**

The Dial-via-Office Forward Service Access Number service parameter provides customers the option to set up a dedicated number for Cisco Unified Mobile Communicator users to dial DVO-F while Cisco Unified Communications Manager receives the calls on a different number (for example, through 1-800 support). The DVO-F service access number can specify a toll-free 1-800 number, which the service provider can map to a local number that reaches the enterprise or to any other alternative number for Cisco Mobile clients to invoke DVO-F calls.

The Dial-via-Office Forward Service Access Number service parameter has the following characteristics:

- Length specifies up to 24 dialable digits.
- Does not specify a partition.

The Dial-via-Office Service Access Number service parameter interacts with the existing Enterprise Feature Access (EFA) DN as follows:

- The EFA DN must be configured to invoke the DVO-F feature. Whether DVO-F service access number is configured or not, the EFA DN terminates the inbound call from the Cisco Unified Mobile Communicator device.

- For the 183 Session in progress message response, the following rules apply:
  - If the Dial-via-Office Forward Service Access Number service parameter number is configured, Cisco Unified Communications Manager sends this alternative number to Cisco Unified Mobility Advantage in SDP.
  - If only EFA DN is configured, Cisco Unified Communications Manager sends the EFA DN to Cisco Unified Mobility Advantage.

- For incoming PSTN calls, the following matching takes place:
  - Called party number gets matched against either the EFA DN or the DVO-F service access number. Either Partial Match or Complete Match takes place. The Partial/Complete Match matches the calling number with the calling number in the original SIP INVITE message that the Cisco Unified Mobility Advantage forwarded to Cisco Unified Communications Manager.
  - Actually this is not accurate. Certainly, the system expects the inbound DVO-F call leg from CUMC to be to (called number) EFA DN or DVO-F service access number. But once the call is received on that number, called number is no longer important. The Partial/Complete Match portion is matching the calling number and the match is not made against the EFA/DVO-F service access number, but the calling number specified in the original SIP INVITE forwarded to Unified CM by CUMA.
  - If a match is found, the voice call correlates with the original SIP Invite, and the Call Await Timer gets stopped. Next, a call gets extended to the called number or target number that the user originally dialed and that the SIP Invite that the Cisco Unified Communications Manager received from Cisco Unified Mobility Advantage contains.
- If no match is found, after the Call Await Timer expires, the call disconnects, and the 503 Service Unavailable message gets sent.

Globalization Support for EFA DN and DVO-F Service Access Number

Both the Enterprise Feature Access Directory Number and the Dial-via-Office Forward Service Access Number support the following dialable digits:

- 0 through 9
- +, which must be preceded by backslash (\). Because backslash is not a dialable digit, it does not count toward the maximum length of 24 digits.
- * and #
- A through D

The preceding special characters can occur in any position.

Use Case Scenarios for Dial-via-Office Forward

See the “Use Case Scenarios for Dial-via-Office Forward” section on page 15-16 for the use case scenarios that Cisco Unified Communications Manager supports with this feature.

Dial-via-Office Forward Call Characteristics

Using the preceding example, the following characteristics apply to a Dial-via-Office Forward call:

- Based on the INVITE SDP parameter “a=setup:active,” Cisco Unified Communications Manager determines that the Cisco Mobile client wants to initiate a DVO-F call.
- The Call Await Timer, which is set to 30 seconds, starts when Cisco Unified Communications Manager sends the 183 Session In Progress message to Cisco Unified Mobility Advantage.
- If the Cisco Unified Communications Manager does not receive a PSTN call from Cisco Unified Mobile Communicator before the Call Await Timer expires, Cisco Unified Communications Manager sends a “503 Service Unavailable” message and clears resources that are associated with the DVO-F Invite.
- When a PSTN call arrives, the following attempts at matching take place:
  - Cisco Unified Communications Manager tries to match the calling party number against known Mobility Identities (MIs) to determine whether the call will get anchored. Cisco Unified Communications Manager performs the match based on the option that is set for the Matching Caller ID with Remote Destination service parameter (either Partial Match or Complete Match).
  - Cisco Unified Communications Manager also tries to match the called party number against the EFA DN or DVO-F service access number and determines whether the call is a DVO-F call.
- After the call gets established, the user can invoke other Cisco Unified Mobility features, such as hold, resume, conference, transfer, and desk pickup.

Example of Dial-via-Office Forward

The following example illustrates the sequence of events that takes place in an instance of Dial-via-Office Forward (DVO-F):

1. User launches the Cisco Unified Mobile Communicator application and enters 2000 as target number.
3. Cisco Unified Communications Manager sends back 183 Session In Progress via the data channel. The SDP parameter specifies the Dial-via-Office Forward service access number or EFA DN.
4. Cisco Unified Mobile Communicator autodials the number that the SDP specifies.
5. Cisco Unified Communications Manager correlates this voice call with the SIP data channel call by comparing the calling party number with the Mobility Identity and by comparing the called party number with the EFA DN or the DVO-F service access number.
6. The call then progresses normally.

**Dial-via-Office Forward Configuration Tips**

The following configuration tips apply when you are configuring the Dial-via-Office Forward feature:

- Cisco Unified Mobile Communicator device must get provisioned with a valid Mobility Identity (MI).
- Cisco Unified Mobile Communicator device must register with Cisco Unified Communications Manager.

If the Cisco Unified Mobile Communicator caller ID that the Cisco Unified Communications Manager receives does not match the provisioned MI completely, perform the following configuration:

- Set the Matching Caller ID with Remote Destination service parameter to Partial Match.
- Specify the number of matched digits in the Number of Digits for Caller ID Partial Match service parameter.

- Make sure the ingress gateway gets configured properly, so the called party number matches either the EFA DN or the DVO-F Service Access Number service parameter.

- If the called party number is expected to match the EFA DN, ensure that the Inbound Calling Search Space for Remote Destination service parameter is set properly as follows:
  - If the Trunk or Gateway Inbound Calling Search Space option is chosen, the EFA DN partition must belong to the trunk or gateway calling search space.
  - If the Remote Destination Profile + Line Calling Search Space option is chosen, the EFA DN partition must belong to the calling search spaces of the Cisco Unified Mobile Communicator device and its enterprise DN.

**Limitations for Dial-via-Office Reverse Callback Feature**

See the “Dial-via-Office Limitations (DVO-R and DVO-F)” section on page 15-18 for a list of limitations that apply to this feature.

**Additional Information**

See the “Related Topics” section on page 15-20.

**Session Resumption**

The Session Resumption feature allows the user to call back to a meeting (after a signal loss) without inputting the meeting ID and password again.

Mobile call failure is very common in the cellular network. For DVO-F calls, the dialed number that is stored on the mobile handset specifies the DVO-F service access number, which is an internally configured DID number. When the user presses **Redial** on the user handset (either by calling the last dialed number from the phone call history or by pressing Call Back if the phone provides such an option), the stored number has already been dialed, so Cisco Unified Communications Manager cannot reach the original target.
Upon implementation of the Session Resumption feature, Cisco Unified Communications Manager stores the target number DN when the DVO-F call initially gets made. If the user presses Redial after a network failure, Cisco Unified Communications Manager receives the call for the DVO-F service access number, which Unified CM replaces with the stored target DN. Thus, the redial request succeeds: either a new call gets extended to the original target, or the original call gets reconnected, depending on whether the original call got released.

**Configuration Details**
The following configuration details apply to the Session Resumption feature.

- The Session Resumption feature uses the setting of the Session Resumption Await Timer service parameter, which you configure in the Service Parameter Configuration window (System > Service Parameters) for the Cisco CallManager service in the Clusterwide Parameters (System - Mobility) pane. The Session Resumption Await Timer service parameter has a default setting of 180 seconds (3 minutes), but can be set to any value between 0 seconds and 300 seconds (5 minutes). Setting the Session Resumption Await Timer service parameter to 0 seconds disables the timer and the Session Resumption feature.

- After the Session Resumption Await Timer expires in the case of a DVO-F call that was interrupted due to network failure, the record of the original target DN for this DVO-F call gets deleted. Any Redial call that is placed after the timer expires gets invoked as an enterprise feature access (EFA) call: the Session Resumption feature does not get triggered.

- If a Redial call gets extended to a busy target DN, the user receives a busy tone.

**Use Case Scenarios**
See the “Use Case Scenarios for Session Resumption” section on page 15-17 for use cases that apply to the Session Resumption feature.

**Limitations for Session Resumption Feature**
See the “Session Resumption Limitation” section on page 15-18 for a list of limitations that apply to this feature.

**Additional Information**
See the “Related Topics” section on page 15-20.

**Use Case Scenarios for Cisco Unified Mobility Features**
The following sections describe the following use case scenarios that Cisco Unified Communications Manager supports for Cisco Unified Mobility features if the required configuration for Cisco Unified Mobility Advantage is also performed:

- Use Case Scenarios for Dial-via-Office Reverse Callback, page 15-16
- Use Case Scenarios for Dial-via-Office Forward, page 15-16
- Use Case Scenarios for Session Resumption, page 15-17

**Additional Information**
See the “Related Topics” section on page 15-20.
Use Case Scenarios for Dial-via-Office Reverse Callback

The Dial-via-Office Reverse Callback feature supports the following use case scenarios:

- Mobile user invokes Dial-via-Office Reverse Callback feature to remote destination and succeeds.
- Mobile user invokes Dial-via-Office Reverse Callback feature to non-remote destination and succeeds.
- Mobile user invokes Dial-via-Office Reverse Callback feature and fails.

Additional Information
See the “Related Topics” section on page 15-20.

Use Case Scenarios for Dial-via-Office Forward

The Dial-via-Office Forward feature supports the following use case scenarios:

1. Enterprise has configured EFA DN only.
   The DVO-F feature succeeds only when the Cisco Unified Mobile Communicator client automatically dials the exact EFA DN and Cisco Unified Communications Manager also receives the identical call party number.

   **Example**
   
   EFA DN = 1239876
   DVO-F Service Access Number service parameter = EMPTY
   Cisco Unified Communications Manager sends 1239876 in 183 message and receives PSTN call to 1239876.

2. Enterprise provides a 1-800 toll-free number for DVO-F calls.
   Enterprise sets up a toll-free number, which may be mapped to an actual number (ring-to number) when the service provider receives the call.
   If the ring-to number gets applied, administrator must configure the toll-free number (for example, 18008889999) by using the Dial-via-Office Forward Service Access Number service parameter and the ring-to number (for example, 4081239876) as the EFA DN.

   **Example**
   
   EFA DN = 1239876 (localized format, depending on service provider)
   DVO-F Service Access Number service parameter = 18008889999
   Cisco Unified Communications Manager sends 18008889999 in 183 Session in progress message and receives PSTN call, which maps to 1239876.

3. Enterprise provides globalized number for DVO-F calls
   Enterprise sets up a globalized access number, which allows its Cisco Unified Mobile Communicator users to invoke the DVO-F calls anywhere in the world without the need to know the international escape code for the country where they are located.
   If the service provider delivers only a localized number, administrator must configure the globalized number (for example, +14081239876) as the DVO-F Service Access Number service parameter and the localized number that Cisco Unified Communications Manager receives (for example, 1239876) as the EFA DN.
Example
EFA DN = 1239876 (localized format, depending on service provider)
DVO-F Service Access Number service parameter = \+14081239876 (requires backslash as escape for + character)
Cisco Unified Communications Manager sends +14081239876 in message 183 Session in progress and receives PSTN call, which maps to 1239876.

Additional Information
See the “Related Topics” section on page 15-20.

Use Case Scenarios for Session Resumption

The Session Resumption feature supports the following use case scenarios.

Session Resumption Use Case 1: New Call to Target
In the case of a DVO-F Redial call where a new call gets made to the target, the following steps take place:
1. User makes DVO-F call, for example, to target DN 1000.
2. While user and target are in a call, a mobile network failure happens.
3. Session Resumption Await Timer starts. Target hears MOH. User does not resume the call on his shared desk line, Desk Pickup Timer (default specifies 30 seconds) expires shortly. Target hangs up.
4. Before Session Resumption Await Timer expires, user called the DVO-F service number.
5. Cisco Unified Communications Manager finds out target (1000) was the last target and makes a new call to the last target (1000 in this example). User and target reconnect.

Session Resumption Use Case 2: Reconnect Existing Call
In the case of a DVO-F Redial call where the existing call to the target gets reconnected, the following steps take place:
1. User makes DVO-F call, for example, to target DN 1000.
2. While user and target are in a call, a mobile network failure happens
3. Session Resumption Await Timer starts. Target hears MOH. User does not resume the call on his shared desk line.
4. Before Desk Pickup Timer (default specifies 30 seconds) expires, user calls the DVO-F service number.
5. Cisco Unified Communications Manager finds that target (1000) was the last target, stops MOH, and reconnects user with the target who was still waiting for user.

Note that no new call is extended to DN 1000: only media switching takes place as the original call to DN 1000 gets reconnected. From the DN 1000 user point of view, when a network failure occurs, DN 1000 first hears MOH. After a few seconds, if the mobile user pressed Redial before the desk pickup timer expires, the original call reconnects and the parties continue the call.

Additional Information
See the “Related Topics” section on page 15-20.
Interactions and Limitations

Be aware that most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features. See the following sections of the “Cisco Unified Mobility” chapter for details of any exceptions:

- Interactions, page 14-28
- Limitations, page 14-30

Additionally, the limitations that apply to features that require Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator functionality are detailed in the following section:

- Limitations, page 15-18

Additional Information
See the “Related Topics” section on page 15-20.

Limitations

This section provides a listing of limitations by feature. The section comprises the following topics:

- Dial-via-Office Limitations (DVO-R and DVO-F), page 15-18
- Session Resumption Limitation, page 15-18

Dial-via-Office Limitations (DVO-R and DVO-F)

The Dial-via-Office Forward (DVO-F) feature specifies these limitations in Cisco Unified Communications Manager:

- Only one outstanding DVO-F call that is getting established from a particular Cisco Unified Mobile Communicator device can be supported at a time.
- DVO-F cannot support simultaneous calls from a single Cisco Unified Mobile Communicator device.
- DVO-F can support two simultaneous DVO-F calls from a single Cisco Unified Mobile Communicator device.
- DVO-F relies on caller ID in the SIP Invite message to correlate a PSTN call with the SIP call:
  - If the calling party number or called party number cannot go through the mobile voice network (for example, GSM), the DVO-F call fails. A standard service provider announcement plays. Cisco Unified Communications Manager sends a 503 Service Unavailable message after the Call Await Timer expires.
  - If Cisco Unified Communications Manager does not receive the calling party number (that is, the Cisco Unified Mobile Communicator user blocks his or her caller ID), the DVO-F call fails. A reorder tone will play. Cisco Unified Communications Manager sends the 503 Service Unavailable message after the Call Await Timer expires.

Session Resumption Limitation

The Session Resumption feature specifies the following limitation:

- Session Resumption feature provides support only for Dial-via-Office Forward calls.

Additional Information
See the “Related Topics” section on page 15-20.
System Requirements

Cisco Unified Mobility, in conjunction with Cisco Unified Mobility Advantage, requires the following software component:

- Cisco Unified Communications Manager 6.0 or later.

Additionally, Cisco Unified Mobility Advantage requires additional software components. See the following documentation for details:


Additional Information

See the “Related Topics” section on page 15-20.

Configuring Cisco Unified Mobility with Cisco Unified Mobility Advantage

The “Configuration Checklist for Cisco Unified Mobility” section on page 14-2 of the “Cisco Unified Mobility” chapter provides an overview checklist of the procedures and steps that are necessary for an administrator to configure Cisco Unified Mobility features that are native to Cisco Unified Communications Manager.

The “Configuring Cisco Unified Mobility” section on page 14-35 of the “Cisco Unified Mobility” chapter provides detailed procedures for each Cisco Unified Communications Manager Administration menu option that must be configured to provision Cisco Unified Mobility features that are native to Cisco Unified Communications Manager. The section covers configuration of the following entities in Cisco Unified Communications Manager Administration:

- Access lists
- Remote destination profiles (You do not need nor use these resources for integration with Cisco Unified Mobility Advantage.)
- Remote destinations
- Mobile voice access media resources (You do not need nor use these resources for integration with Cisco Unified Mobility Advantage.)
- H.323 and SIP gateways for mobile voice access (You do not need nor use these resources for integration with Cisco Unified Mobility Advantage.)
- Enterprise feature access two-stage dialing (Integration with Cisco Unified Mobility Advantage does not require configuration of this feature; however, configuration of the Enterprise Feature Access DID is needed because this DID provides the caller ID that Cisco Unified Communications Manager sends for Dial-via-Office callback call legs.)
- Mobility Enterprise Feature configuration
- Mobility profiles
- Handoff mobility configuration
Mobility softkeys
End users use the Cisco Unified CM User Options windows to further configure or modify the Cisco Unified Mobility settings that apply to their mobile phones.

For the steps that are necessary to configure Cisco Unified Mobility Advantage with Cisco Unified Communications Manager to provide Cisco Unified Mobility features that require Cisco Unified Mobility Advantage, see the following documentation:


**Tip**
Before you configure Cisco Unified Mobility, review the “Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage” section on page 15-2.

**Additional Information**
See the “Related Topics” section on page 15-20.

**Related Topics**

- Configuration Checklist for Cisco Unified Mobility with Cisco Unified Mobility Advantage, page 15-2
- Introducing Cisco Unified Mobility with Cisco Unified Mobility Advantage, page 15-4
  - Definitions, page 15-5
  - List of Cisco Unified Mobility Features with Cisco Unified Mobility Advantage, page 15-5
  - Cisco Unified Mobile Communicator, page 15-7
  - Dial-via-Office Reverse Callback, page 15-10
  - Dial-via-Office Forward, page 15-11
  - Use Case Scenarios for Cisco Unified Mobility Features, page 15-15
- Interactions and Limitations, page 15-18
  - Limitations, page 15-18
- System Requirements, page 15-19
- Configuring Cisco Unified Mobility with Cisco Unified Mobility Advantage, page 15-19
- End User Configuration, *Cisco Unified Communications Manager Administration Guide*
- Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
- Licenses for Cisco Unified Mobility, *Cisco Unified Communications Manager Features and Services Guide*

**Additional Cisco Documentation**

- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Security Guide*
• Applicable Cisco Unified IP Phone User Guides
• Applicable Cisco Unified IP Phone Administration Guides
• Applicable Cisco Unified Mobile Communicator end-user documentation
Cisco Mobile VoiP Clients

Cisco Unified Communications Manager provides certain functionality for Cisco Mobile VoiP Clients that connect directly with Cisco Unified Communications Manager. This chapter discusses the features and the required configurations.

Beginning in Release 8.5(1) of Cisco Unified Communications Manager, Cisco Mobile VoiP Clients register directly with Cisco Unified Communications Manager and no longer need to register with the Cisco Unified Mobility Advantage server.

The name “Cisco Mobile” has also been used for several mobility clients that require a Cisco Unified Mobility Advantage server. Those clients are unrelated to the clients that this chapter discusses. For more information about those clients, see the “Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator Integration” chapter.

Cisco Mobile is the name given to a family of clients that run on mobile devices. Different Cisco Mobile clients offer different features. Features may include the following:

- Direct connection from Cisco Unified Communications Manager to mobile client without proxy server
- Dial-via-Office (DVO) optimization settings for toll reduction
- Enable/disable Mobile Connect from mobile phone
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward
- Ability to transfer active Dial-via-Office calls between the mobile device and the desktop phone

Complete configuration details about configuring the Cisco Mobile VoiP Clients, see the following documentation:


See the end-user guide for a particular Cisco Unified IP Phone for procedures that end users follow to configure the Cisco Unified Mobility settings for their phones by using the Cisco Unified CM User Options windows.

This chapter includes information on the following topics:

- Configuration for Cisco Mobile VoiP Clients, page 16-2
- Introducing Cisco Mobile VoiP Clients, page 16-2
  - Definition, page 16-3
Complete configuration instructions for Cisco Mobile VoIP Clients are found in the following location:


For more information on Cisco Unified Mobility features that are available upon configuration of the Cisco Unified Mobility Advantage server, see the “List of Cisco Mobile VoIP Client Features” section on page 16-3.

Introducing Cisco Mobile VoIP Clients

Be aware that special configuration in Cisco Unified Communications Manager Administration is required for features that Cisco Mobile VoIP Clients provide.

This section discusses the following topics:

• Definition, page 16-3
• List of Cisco Mobile VoIP Client Features, page 16-3
• Direct Connection from Cisco Unified Communications Manager to Mobile Client Without Proxy Server, page 16-4
• DVO Optimization Settings for Toll Reduction, page 16-5
• Enable/Disable Mobile Connect From Mobile Phone, page 16-6

Additional Information

See the “Related Topics” section on page 16-7.
Definition

Table 16-1 provides the definition of a term that relates to Cisco Unified Mobility with Cisco Mobile VoIP Clients.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Mobile 8.x</td>
<td>These direct-connect dual-mode clients support voice-over-Wi-Fi (for costing savings) in addition to cellular. They connect to Cisco Unified Communications Manager directly without the need of a proxy server.</td>
</tr>
</tbody>
</table>

Additional Information
See the “Related Topics” section on page 16-7.

List of Cisco Mobile VoIP Client Features

This section provides a list of Cisco Unified Mobility features that are available to mobile phone users when the Cisco Mobile VoIP Client has been configured. This material discusses configuration within Cisco Unified Communications Manager Administration.

The following entities and features require configuration of Cisco Unified Mobility in Cisco Unified Communications Manager Administration:

- **Direct connection from Cisco Unified Communications Manager to mobile client without proxy server**—This feature provides server-side support for Cisco Mobile VoIP Clients to connect to Cisco Unified Communications Manager directly and thus eliminate Cisco Unified Mobility Advantage in the deployment. Cisco Unified Communications Manager adjusts to support direct connection with the Cisco Mobile VoIP Client. See the “Direct Connection from Cisco Unified Communications Manager to Mobile Client Without Proxy Server” section on page 16-4 for a detailed discussion.

- **DVO Optimization Settings for Toll Reduction**—This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. Administrators assign a profile based on the user location and any other available information. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call. See the “DVO Optimization Settings for Toll Reduction” section on page 16-5 for a detailed discussion.

- **Enable/Disable Mobile Connect From Mobile Phone**—This feature allows the Cisco Mobile VoIP Client to change the Mobile Connect status dynamically and keep the Mobile Connect Status between Cisco Unified Communications Manager and the client in sync. This feature provides the flexibility to the end user: the end user can change the user Mobile Connect status from the user mobile phone, not just from the GUI website. See the “Enable/Disable Mobile Connect From Mobile Phone” section on page 16-6 for a detailed discussion. See the “Methods for Enabling and Disabiling Mobile Connect” section on page 14-8 of the “Cisco Unified Mobility” chapter for a list of the various methods for updating Mobile Connect status.

The following features, which were originally part of Cisco Unified MobilityManager, now reside in Cisco Unified Communications Manager:

- **Mobile Connect**—See the “Cisco Unified Mobility” chapter for details.

- **Desktop Call Pickup**—See the “Cisco Unified Mobility” chapter for details.
• Access List—See the “Cisco Unified Mobility” chapter for details.
Cisco Unified Communications Manager also supports the following Cisco Unified Mobility features:
• Midcall Enterprise Feature Support Using DTMF—See the “Cisco Unified Mobility” chapter for details.
• Dual-mode Phone Support—See the “Cisco Unified Mobility” chapter for details.
• Manual Handoff of Calls on a Dual-mode Phone—See the “Cisco Unified Mobility” chapter for details.
• Time-of-Day Access—See the “Cisco Unified Mobility” chapter for details.
• Directed Call Park via DTMF—See the “Cisco Unified Mobility” chapter for details.
• SIP URI Dialing—See the “Cisco Unified Mobility” chapter for details.
See the “Other Benefits of Cisco Unified Mobility Features” section on page 14-7 for a discussion of other benefits of Cisco Unified Mobility features, such as simultaneous desktop ringing, single enterprise voice mailbox, system remote access, caller ID, remote on/off control, call tracing, security and privacy for Mobile Connect calls, and smartphone support.

Additional Information
See the “Related Topics” section on page 16-7.

Direct Connection from Cisco Unified Communications Manager to Mobile Client Without Proxy Server

Registration between the Cisco Mobile VoIP Client and Cisco Unified Communications Manager takes place over a separate TCP port. (The shared or pooled connection that was used by the Cisco Unified Mobility Advantage server is not used.) Keepalive messages between the Cisco Mobile VoIP Client and Cisco Unified Communications Manager remain the same as those passed between Cisco Unified Communications Manager and Cisco Unified Mobility Advantage. Cisco Mobile VoIP Client registration with Cisco Unified Communications Manager introduces no new alarms, and registration takes place over the SIP channel.

If the client is running on the iPhone and the Cisco Mobile VoIP Client is unable to complete the SIP dialog, the Cisco Unified Communications Manager retains the PSTN call. (The PSTN call does not drop even if the SIP stat times out.) For example, if Cisco Unified Communications Manager does not receive an ACK message after it sends a 200 OK message, the PSTN call gets retained.

Limitation for Direct Connection From Cisco Unified Communications Manager to Mobile Client
This feature specifies the following limitation:
• If the SIP dialog between Cisco Unified Communications Manager and the Cisco Mobile VoIP Client is not complete, the dialog cannot be used for further midcall feature invocations. The user can, however, invoke midcall features through the DTMF interface.

Additional Information
See the “Related Topics” section on page 16-7.
DVO Optimization Settings for Toll Reduction

This feature supports a pre-configured policy to determine which mobile origination call (DVO-R or DVO-F) yields the least cost to the enterprise; this determination is typically based on locations. This feature benefits the mobile user by allowing the user to find the least cost when making a mobile call. The DNIS pool provides a list of Direct Inward Dialing (DID) numbers so that the user, if roaming, can choose a non-international number for the mobile call. Least cost routing negotiates with Cisco Unified Communications Manager to determine whether DVO-R or DVO-F generates the least cost, then chooses the less costly method for making the call.

Reasons for Least Cost Routing and DNIS Pool

The following reasons make this feature desirable:

- Administrator can decide upon the DVO call type, DVO-F or DVO-R, for least cost call routing. In certain regions and with certain service providers, DVO-F can be more economical for mobile users; in other regions, DVO-R can be more economical. For example, in regions where incoming calls are free for mobile phone users, configuring a DVO-R call for mobile phone users achieves least cost call routing.

- Scalability—Multiple users in a given region can use a single mobility profile, which comprises region, service provider, location, and so forth. Here, “users” refers to the clients under actual end users. The administrator does not need to create a mobility profile for each end user.

- Single DID within a cluster for all DVO-F calls—For such DVO-F calls, the client makes an incoming call to Cisco Unified Communications Manager by using a particular DID.

- Multisite cluster—For a multisite cluster, a client in cluster A (such as the UK) uses the DID of cluster B (such as San Jose) for DVO-F calls, which incurs costs.

- DVO-R—Trunk allows calls that originate from a local DID. At times, when a client makes an outgoing DVO-R call, the client trunk may not allow an outgoing call if the caller ID does not lie in a specific range. For example, if a UK client invokes DVO-R, the callback call from the trunk at the San Jose cluster shows 408. When this call reaches the UK, the service provider trunk may not recognize the 408 and therefore not allow the call. Therefore, the caller IDs need to specify the local identifiable values.

Characteristics of DVO Optimization Settings for Toll Reduction

This feature involves the use of mobility profiles, which the administrator configures by using the Call Routing > Mobility > Mobility Profile menu path in Cisco Unified Communications Manager Administration. See the “Mobility Profile Configuration” section on page 14-58 for additional details about mobility profiles.

The DVO Optimization Settings for Toll Reduction feature does not change the alternate callback mechanism that DVO-R calls use: the client continues to control alternate callback.

Limitation of DVO Optimization Settings for Toll Reduction

The DVO Optimization Settings for Toll Reduction feature specifies the following limitation:

- Least Cost Routing (LCR) rules are applied after application dial rules. Called party transformations and call forward scenarios do not get considered for LCR.

Additional Information

See the “Related Topics” section on page 16-7.
Enable/Disable Mobile Connect From Mobile Phone

Prior to Release 8.5(1) of Cisco Unified Communications Manager, Cisco Unified Communications Manager sent Mobile Connect status updates to the Cisco Unified Mobile Communicator client via Cisco Unified Mobility Advantage by AXL messages. Direct SIP messages between the Cisco Mobile VoIP Client and Cisco Unified Communications Manager now allow the client to change the client Mobile Connect status.

Beginning with Release 8.5(1) of Cisco Unified Communications Manager, the Cisco Mobile VoIP Client can update its Mobile Connect status directly.

Additional Information

See the “Related Topics” section on page 16-7.

Interactions and Limitations

Be aware that most standard Cisco Unified Communications Manager features are fully compatible with Cisco Unified Mobility features. See the following sections of the “Cisco Unified Mobility” chapter for details of any exceptions:

- Interactions, page 14-28
- Limitations, page 14-30

Additional Information

See the “Related Topics” section on page 16-7.

System Requirements

See the following documentation for detailed system requirements:

Release Notes for Cisco Mobile at

Additional Information

See the “Related Topics” section on page 16-7.

Configuring Cisco Mobile VoIP Clients

Complete configuration details about configuring the Cisco Mobile VoIP Clients, see the following documentation:

- Configuration guides for Cisco Mobile VoIP Clients at this URL:

Additional Information

See the “Related Topics” section on page 16-7.
Related Topics

- Configuration for Cisco Mobile VoIP Clients, page 16-2
- Introducing Cisco Mobile VoIP Clients, page 16-2
  - Definition, page 16-3
  - List of Cisco Mobile VoIP Client Features, page 16-3
  - Direct Connection from Cisco Unified Communications Manager to Mobile Client Without Proxy Server, page 16-4
  - DVO Optimization Settings for Toll Reduction, page 16-5
  - Enable/Disable Mobile Connect From Mobile Phone, page 16-6
- Interactions and Limitations, page 16-6
- System Requirements, page 16-6
- Configuring Cisco Mobile VoIP Clients, page 16-6
- End User Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Licenses for Cisco Unified Mobility, Cisco Unified Communications Manager Features and Services Guide

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Security Guide
- Applicable Cisco Unified IP Phone User Guides
- Applicable Cisco Unified IP Phone Administration Guides
- Applicable Cisco Mobile VoIP Client installation, upgrade, and end-user documentation
Cisco Web Dialer

Cisco Web Dialer, used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications.

This chapter provides the following information about Cisco Web Dialer:

- Configuration Checklist for Cisco Web Dialer, page 17-1
- Introducing Cisco Web Dialer, page 17-2
- Redundancy, page 17-3
- System Requirements for Cisco Web Dialer, page 17-4
- Interactions and Restrictions, page 17-4
- Installing and Activating Cisco Web Dialer, page 17-5
- Configuring Cisco Web Dialer, page 17-6
- Related Topics, page 17-14

**Configuration Checklist for Cisco Web Dialer**

Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager server and used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

Table 17-1 provides a configuration checklist for Cisco Web Dialer. For more information, see the “Related Topics” section on page 17-14.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Activate the Cisco Web Dialer service.</td>
<td>Installing and Activating Cisco Web Dialer, page 17-5</td>
</tr>
<tr>
<td>Step 2: Configure the Webdialer servlet.</td>
<td>Setting Service Parameters for the Webdialer Servlet, page 17-6</td>
</tr>
<tr>
<td>Step 3: Configure Cisco Web Dialer as an application server in the Application Server window in Cisco Unified Communications Manager Administration.</td>
<td>Configuring Cisco Web Dialer in the Application Server Window, page 17-8</td>
</tr>
</tbody>
</table>
Introducing Cisco Web Dialer

Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager server and used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

Cisco Web Dialer includes the following main components:

- **Webdialer Servlet, page 17-2**
- **Redirector Servlet, page 17-3**

### Webdialer Servlet

The Webdialer servlet, a Java servlet, allows Cisco Unified Communications Manager users in a specific cluster to make and complete calls, as well as to access their phone and line configuration.

An application can interact with the Webdialer servlet through two interfaces:

- The SOAP over HTTPS interface—This interface that is based on the Simple Object Access Protocol (SOAP) gets used to develop desktop applications such as Microsoft Outlook Add-in and SameTime Client Plug-in. Developers can use the isClusterUserSoap interface to design multicluster applications that require functionality similar to a Redirector servlet.

### Table 17-1 Cisco Web Dialer Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 Add each user that you want to use Web Dialer to the Standard End User Group for Cisco Unified Communications Manager.</td>
<td>Adding Users to the Standard Cisco Unified Communications Manager End Users Group, page 17-12</td>
</tr>
<tr>
<td>Step 5 Determine which language Web Dialer displays by setting the locale field in the Cisco Unified CM User Options menu.</td>
<td>Configuring Web Dialer for the Local Language, page 17-10</td>
</tr>
<tr>
<td>Step 6 (Optional) Configure the Redirector servlet.</td>
<td>Configuring the Redirector Servlet (Optional), page 17-11</td>
</tr>
<tr>
<td>Step 7 (Optional) Configure the application dial rules for multiple cluster applications.</td>
<td>Configuring Application Dial Rules (Optional), page 17-11</td>
</tr>
<tr>
<td>Step 8 (Optional) Create a proxy user.</td>
<td>Creating a Proxy User (Optional), page 17-12</td>
</tr>
<tr>
<td>Step 9 (Optional) Configure Cisco Web Dialer trace settings.</td>
<td>Trace Settings (optional), page 17-14</td>
</tr>
<tr>
<td>Step 10 Configure Cisco Web Dialer alarms.</td>
<td>Related Topics, page 17-14</td>
</tr>
</tbody>
</table>

Cisco Unified Serviceability Administration Guide

## Introducing Cisco Web Dialer

Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager server and used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications. For example, Cisco Web Dialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

Cisco Web Dialer includes the following main components:

- **Webdialer Servlet, page 17-2**
- **Redirector Servlet, page 17-3**
Redundancy

- HTML over HTTPS interface—This interface that is based on the HTTPS gets used to develop web-based applications. Developers who use this interface can use the Redirector servlet for designing multicloud applications.

Redirector Servlet

The Redirector servlet, a Java-based Tomcat servlet, finds the Cisco Unified Communications Manager cluster for a request that a Cisco Web Dialer user makes. It redirects that request to the specific Cisco Web Dialer server that is located in that user Cisco Unified Communications Manager cluster. Availability of the Redirector servlet occurs only for multicloud applications and only for applications that are developed by using HTML over HTTPS interfaces.

Example of Cisco Web Dialer Using the Redirector Servlet

For example, consider three clusters, each one in a single city such as San Jose (SJ-CM), Dallas (D-CM), and New York (NY-CM). Each cluster contains three Cisco Unified Communications Manager servers with Webdialer servlets that have been configured for Cisco Unified Communications Manager servers SJ-CM1, D-CM2, and NY-CM3.

The system administrator configures the Webdialer servlets on any Cisco Unified Communications Manager server by entering the IP address of that specific Cisco Unified Communications Manager server in the List of Web Dialers service parameter (see the “Setting Service Parameters for the Webdialer Servlet” section on page 17-6). For information on configuring the Webdialer servlet and the Redirector servlet, see the “Configuring the Webdialer Servlet” section on page 17-6 and the “Configuring the Redirector Servlet (Optional)” section on page 17-11.

When a user who is located in San Jose clicks on a telephone number in the corporate directory search window that Cisco Web Dialer enables, the following actions happen:

1. The user application (client) sends an initial makeCall HTTPS request to the Redirector servlet.

2. If this request is received for the first time, the Redirector servlet reads the Cisco Web Dialer server cookie and finds it empty.

   For a repeat request, the Redirector servlet reads the IP address of the Cisco Web Dialer server that previously serviced the client and sends a isClusterUser HTTPS request only to that server.

3. The Redirector servlet sends a response that asks for information, which results in the authentication dialog box opening for the user.

4. The user enters the Cisco Unified Communications Manager user ID and password and clicks the Submit button.

5. The Redirector servlet reads only the user identification from this information and sends an isClusterUser HTTPS request to each Cisco Web Dialer server that the system administrator has configured.

6. The Redirector servlet redirects the original request from the user to SJ-CM1.

Additional Information

See the “Related Topics” section on page 17-14.

Redundancy

Because redundancy is important for applications that are running in a multicloud environment, this section describes one method to achieve that redundancy.
If a single Redirector servlet is supporting multiple Cisco Web Dialers in a multicluster environment, it provides a single point of failure. For example, in Figure 17-1, a Redirector servlet runs on the San Jose cluster and also services the New York and Dallas clusters. If this Redirector servlet fails to run on the San Jose cluster, the users who are serviced by all three clusters cannot use Cisco Web Dialer.

To avoid this single point of failure, configure Redirector servlets for each cluster. If the directory search window points to a URL such as https://sanjoseclustercompany.com:8443/webdialer/Redirector, change that URL to a virtual link such as https://webdialer-service.company.com/webdialer/Redirector. This virtual link points to a virtual machine that is using a Cisco DistributedDirector. All the Redirector servlets operate behind this virtual link.

For more information on installing and configuring Cisco DistributedDirector, see the suite of documents for Cisco DistributedDirector.

**Additional Information**

See the “Related Topics” section on page 17-14.

## System Requirements for Cisco Web Dialer

Cisco Web Dialer requires the following software components:

- Cisco Unified Communications Manager 5.0(2) or later
- Cisco Unified IP Phones that CTI supports

To configure your company directory search window for Cisco Web Dialer or the Cisco Unified Communications Manager directory search window, you must

- Install and configure Cisco Unified Communications Manager.
- Configure Cisco Web Dialer.

You can launch Cisco Web Dialer from the Directory window, in Cisco Unified CM User Options. For example, you could access a URL similar to the following one:

https://<IP address of Cisco Unified Communications Manager server>:8443/ccmuser/showhome.do.

For documentation on installing and configuring Cisco Unified Communications Manager, see the “Related Topics” section on page 17-14.

## Interactions and Restrictions

The following sections describe the interactions and restrictions for Cisco Web Dialer:

- Interactions, page 17-4
- Restrictions, page 17-5

### Interactions

The following interactions apply to Cisco Web Dialer:

- When using Client Matter Codes (CMC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.
• When using Forced Authorization Codes (FAC), the user must enter the proper code at the tone; otherwise, the IP phone disconnects, and the user receives reorder tone.
• Cisco Web Dialer uses change notifications on the ApplicationDialRule database table to track and use the updated dial rules.

Restrictions
Cisco Web Dialer supports phones that run Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) that Cisco Computer Telephony Integration (CTI) supports.

Note
Cisco Web Dialer supports only the 7970/71 and 7961/41 IP phone models that run SIP.

Additional Information
See the “Related Topics” section on page 17-14.

Installing and Activating Cisco Web Dialer
Cisco Web Dialer automatically installs on the server on which you installed Cisco Unified Communications Manager.

Perform the following procedure to activate Cisco Web Dialer on the Cisco Unified Communications Manager server.

Procedure

Step 1 From the navigation area of the Cisco Unified Communications Manager application, choose Cisco Unified Serviceability and click Go.

Step 2 Choose Tools > Service Activation.

Step 3 Choose the Cisco Unified Communications Manager server that is listed in the Servers drop-down list box.

Step 4 From CTI Services, check the check box next to Cisco Web Dialer Web Service.

Step 5 Click Save.

Note
You must also activate and start the CTI Manager service for Cisco Web Dialer to function properly. To ensure that the CTI Manager service is started, from Cisco Unified Serviceability, choose Tools > Control Center - Feature Services.

Additional Information
See the “Related Topics” section on page 17-14.
Configuring Cisco Web Dialer

This section contains the following information:

- Configuring the Webdialer Servlet, page 17-6
- Setting Service Parameters for the Webdialer Servlet, page 17-6
- Configuring the Application User, page 17-9
- Configuring Web Dialer for the Local Language, page 17-10
- Configuring the Redirector Servlet (Optional), page 17-11

Tip
Before you configure Cisco Web Dialer, review the “Configuration Checklist for Cisco Web Dialer” section on page 17-1.

Configuring the Webdialer Servlet

To configure the Webdialer servlet

- Activate the Cisco Web Dialer service. See the “Installing and Activating Cisco Web Dialer” section on page 17-5.
- Set trace settings (optional). See the “Trace Settings (optional)” section on page 17-14.
- Set the Cisco Web Dialer service parameters. See the “Setting Service Parameters for the Webdialer Servlet” section on page 17-6.
- Configure application user.

Additional Information
See the “Related Topics” section on page 17-14.

Setting Service Parameters for the Webdialer Servlet

Cisco Unified Communications Manager provides the following service parameters for the Webdialer servlet:

- CAPF Profile Instance ID for Secure Connection to CTI Manager—This parameter specifies the Instance Id of the Application CAPF Profile for Application User WDSecureSysUser that this Cisco Web Dialer server will use to open a secure connection to CTI Manager.
- Primary Cisco CTIManager—Enter the IP address of the primary Cisco CTIManager.
  The default IP address of the Cisco CTI Manager specifies 127.0.0.1, which is the local host server that is used to set up Cisco Web Dialer.
  The maximum length specifies 15 digits.
- Backup Cisco CTIManager—Enter the IP address of the backup Cisco CTIManager. The maximum length specifies 15 digits. No IP address implies that no backup Cisco CTIManager exists.
• User Session Expiry (in hours)—Enter the duration, in hours, for which the user login session is valid.

A default value of 0 indicates that the login session is valid for an indefinite time, until Cisco Web Dialer Web Service is restarted the next time.

The minimum length specifies 0 hours, and the maximum length specifies 168 hours.

• Maximum Concurrent Call Requests—This parameter specifies the maximum number of concurrent WebDialer call requests that the WebDialer service can accept.

For example:

- MCS 7825H2 supports a maximum of 2 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 3 to allow callers to initiate and disconnect calls as needed.

- MCS 7845H2 supports a maximum of 4 calls per second. Cisco recommends setting the MaxConcurrentCallRequests (MCCR) value to 8 to allow callers to initiate and disconnect calls as needed.

Enter a lower value if RTMT alerts, alarms, or performance counters suggest the hardware associated with WebDialer is being overutilized (for example, spikes in CPU, entering Code Yellow). Enter a higher value to allow more simultaneous WebDialer call requests. Be aware that a higher value can add more load to the CPU.

The maximum value specifies 8.

The default value specifies 3.

• Duration of End Call Dialog (in seconds)—Enter the duration, in seconds, to display the dialog to end a call. This dialog indicates that the user must end the call if the user dialed out in error.

The default value specifies 15 seconds, with a maximum value of 60 seconds and a minimum value of 10 seconds.

To disable the Duration of End Call Dialog service parameter, the user checks the Disable Auto-Close check box in the User Options window. If the Disable Auto-Close check box is checked, the End Call dialog does not close automatically, and the Hangup button returns the user to the Make Call window.

• Apply Application Dial Rules on Dial—Default specifies True. If you do not need Cisco Web Dialer to use application dial rules, change the setting to False.

• CTI Manager Connection Security Flag—This clusterwide parameter indicates whether security for the Cisco Web Dialer service CTI Manager connection gets disabled or complies with the security mode of the cluster. If security is enabled, Cisco Web Dialer opens a secure connection to CTI Manager by using the Application CAPF profile that is configured in Application CAPF Profile Instance Id for Secure Connection to CTI Manager parameter.

All changes require a restart of the Cisco Web Dialer service for the changes to take effect.

Use the following procedure initially to set or modify existing service parameters for the Webdialer servlet.

**Procedure**

**Step 1** Choose System > Service Parameters.
Step 2 From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure Cisco Web Dialer service parameters.

Step 3 From the Service drop-down list box, choose the Cisco Web Dialer Web Service.

Default values already exist for the parameters Primary Cisco CTIManager, Duration of End Call Dialog, User Session Expiry (InHours), and Apply Application Dial Rules (True). Enter new values if your application requires them.

The parameter Backup Cisco CTIManager does not have any default values that are assigned to it. Enter values for this parameter if your application requires a backup Cisco CTIManager.

Step 4 For new parameter values to take effect, restart the Cisco Web Dialer Web Service.

Additional Information
See the “Related Topics” section on page 17-14.

Configuring Cisco Web Dialer in the Application Server Window

Instead of configuring the List of WebDialers service parameter, which limits the number of characters that you can enter, you can configure the WebDialer servers in the Application Server Configuration window in Cisco Unified Communications Manager Administration. To access the Application Server Configuration window, choose System > Application Server in Cisco Unified Communications Manager Administration. Cisco Web Dialer appears as one of the options in the Application Server Type drop-down list box.

After you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service.

Tip
You can configure either the List of WebDialers service parameter or the Cisco Web Dialer application server through the Application Server Configuration window. If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service. You can access the Service Parameter Configuration window by choosing System > Service Parameters in Cisco Unified Communications Manager Administration.

If you configured the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service before the upgrade to Cisco Unified Communications Manager 8.0(2) (or higher), the configured list of Web Dialers gets automatically migrated during the upgrade.

If you install Cisco Unified Communications Manager and plan to use Cisco Web Dialer, configure the Cisco Web Dialer application server in the Application Server Configuration window. You do not need to configure the List of WebDialers field in the Service Parameter Configuration window if you configure the application server in the Application Server Configuration window.
Configuring the Application User

The Web Dialer needs a CTI connection to make and end calls. The Web Dialer uses the application user and password that are required to create a CTI provider. (The database stores this value as application user and the system retrieves it from there.) To secure a TLS connection to CTI, see the “Secure TLS Connection to CTI” section on page 17-9.

Secure TLS Connection to CTI

Cisco Web Dialer supports a secure (TLS) connection to CTI. Obtain the secure connection by using the “WDSecureSysUser” application user.

Note
You must configure a CAPF profile, in the Application User CAPF Profile Configuration windows in Cisco Unified Communications Manager Administration, that is configured for the instance ID for application user WDSecureSysUser to obtain a secure connection. If you enable security from the Service Parameter Configuration window, the Cisco Web Dialer will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance ID for Secure Connection to CTI Manager” service parameters for the secure connection to succeed. See “Application User CAPF Profile Configuration” and “Service Parameter Configuration” in the Cisco Unified Communications Manager Administration Guide.

Perform the following procedure to configure the application user.

Procedure

Step 1 Choose User Management > Application User.
The Find and List Application Users window displays.

Step 2 Click Find.

Step 3 From the Find and List Application Users window, click WDSysUser or WDSecureSysUser.

Note To configure a CAPF profile, see “Application User CAPF Profile Configuration” in the Cisco Unified Communications Manager Administration Guide for general information and to the Cisco Unified Communications Manager Security Guide for details.

Note You can change the password that is associated with the WDSysUser. The application obtains the new password from the database.

Additional Information
See the “Related Topics” section on page 17-14.
Configuring Web Dialer for the Local Language

Cisco Unified Communications Manager gives precedence to languages that are set up in the client browser; for example, Microsoft Internet Explorer (see Figure 17-1). To change the language that the client displays, use the browser settings (not the Locale field in the Cisco Unified CM User Options menu). Conversely, Cisco Web Dialer gives precedence to the locale that is configured in the Cisco Unified CM User Options menu. Cisco Web Dialer accesses locales in the following ways:

- You can configure a Cisco Web Dialer user for a locale from the Cisco Unified CM User Options menu; for example, Japanese. When the user logs in to Web Dialer, the Web Dialer preferences window displays in Japanese. The user can change the language to the browser language; for example, by using Microsoft Internet Explorer. Cisco Web Dialer recognizes the browser language only in the format ll_CC. For example, the Japanese locale gets defined as ja_JP.

Note
If the Japanese language displays incorrectly when you use Microsoft Windows, ensure that the Unicode font is installed on your machine.

- You can configure a Cisco Web Dialer (Locale field is set to None in the Cisco Unified CM User Options menu). When the user logs in to Web Dialer, the Web Dialer preferences window displays in English. To change the language of the browser, the user must add a user-defined locale in the browser (using the format of ll_CC). For example, the Japanese locale gets defined as ja_JP.

Figure 17-1 Locale Settings in Microsoft Internet Explorer

![Locale Settings in Microsoft Internet Explorer](image)

See the documentation that came with your browser for information on how to change a user-defined locale. See Customizing Your Cisco Unified IP Phone on the Web for information on how to set the locale in the Cisco Unified CM User Options menu.

Additional Information
See the “Related Topics” section on page 17-14.
Partition Support

Cisco Web Dialer includes partition information, provided by JTAPI, as well as line information. The following list comprises the different available configurations:

- Lines with the same DN: Cisco Web Dialer handles different partition as different lines.
- Lines with the same DN: Cisco Web Dialer handles same partition and different devices as shared lines.
- Lines with the same DN: Cisco Web Dialer does not support same partition and in same device.

Additional Information
See the “Related Topics” section on page 17-14.

Configuring the Redirector Servlet (Optional)

Configure the Redirector servlet only if your applications require multiple clusters. Perform the following procedure to configure the Redirector servlet.

Procedure

**Step 1** Choose **System > Service Parameters**.
**Step 2** From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure the Redirector Servlet.
**Step 3** From the Service drop-down list box, choose the Cisco Web Dialer Web Service.
**Step 4** For the parameter, *List of Web Dialers*, enter new values that your application requires. See the “Setting Service Parameters for the Webdialer Servlet” section on page 17-6 for a description of this service parameter.

Additional Information
See the “Related Topics” section on page 17-14.

Configuring Application Dial Rules (Optional)

Ensure that the application dial rules are configured for multiple cluster applications of Cisco Web Dialer.

For information on configuring these application dial rules, see the “Application Dial Rule Configuration” section on page 27-1 in the *Cisco Unified Communications Manager Administration Guide* for dial rule design and error checking.

**Note**
Cisco Web Dialer must pick up the dial rule change without a restart.

Additional Information
See the “Related Topics” section on page 17-14.
Adding Users to the Standard Cisco Unified Communications Manager End Users Group

For users to use the Cisco Web Dialer links in the User Directory windows in Cisco Unified Communications Manager, you must add each user to the Standard Cisco Unified Communications Manager End Users Group. The following procedure describes how to add users to this group.

Procedure

**Step 1** Choose **User Management > User Group**.
The Find and List User Group window displays.
Click **Find**.

**Step 2** Click the **Standard CCM End Users** link.

**Step 3** The User Group Configuration window displays.

**Step 4** Click **Add End Users to Group**.
The Find and List Users window displays.

**Step 5** Click **Find**. You can enter criteria for a specific user.

**Step 6** Check the check box next to the users that you want to add to the user group and click **Add Selected**.

**Note** If you want to add all users in the list of users, click **Select All** and then **Add Selected**.

The users display in the Users in Group table on the User Group Configuration window.

**Additional Information**
See the “Related Topics” section on page 17-14.

Creating a Proxy User (Optional)

Create a proxy user if you are using the makeCallProxy HTML over HTTP interface to develop an application for using Cisco Web Dialer. For information on the makeCallProxy interface, see the makeCallProxy section in the Cisco Web Dialer API Reference Guide.

You can enable authentication proxy rights for either an existing user or a new user.

**Authentication Proxy Rights for Existing User**
Perform the following procedure to enable authentication proxy rights for an existing user.

**Procedure**

**Step 1** Choose **User Management > User Group**.
The Find and List User Group window displays.
Click **Find**.
Configuring Cisco Web Dialer

Step 2 Click the **Standard EM Authentication Proxy Rights** link.
The User Group Configuration window displays.

Step 3 Click **Add End Users to Group**.
The Find and List Users window displays.
Click **Find**. You can also add a criteria for a specific user.

Step 4 Choose the user to which you want to add proxy rights and click **Add Selected**.

```
Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.
```

The user displays in the Users in Group table on the User Group Configuration window.

**Authentication Proxy Rights for New User**
Perform the following procedure to enable authentication proxy rights for a new user.

**Procedure**

Step 1 Choose **User Management > End User**.
Step 2 Click **Add New**.
Step 3 Enter the following mandatory fields:
**Last Name**: **User ID**: **Password**: **Confirm Password**: **PIN**; and **Confirm PIN**.
Step 4 Click **Save**.
Step 5 Choose **User Management > User Group**.
The Find and List User Group window displays.
Step 6 Click the **Standard EM Authentication Proxy Rights** link.
The User Group Configuration window displays.
Step 7 Click **Add End Users to Group**.
The Find and List Users window displays.
Step 8 Click **Find**. You can also enter criteria for a specific user.
Step 9 Choose the user to which you want to add proxy rights and click **Add Selected**.

```
Note If you want to add all the users in the list, click **Select All** and then click **Add Selected**.
```

The user displays in the Users in Group table on the User Group Configuration window.

**Additional Information**
See the “**Related Topics**” section on page 17-14.
Trace Settings (optional)

You can configure trace settings from Cisco Unified Serviceability Administration. Use the following CLI commands to access the trace files:

```
file get activelog tomcat/logs/webdialer/log4j
file get activelog tomcat/logs/redirector/log4j
```

You can use the Real Time Monitoring Tool (RTMT) to collect traces.

---

**Note**

The same trace settings apply to both Cisco Web Dialer and Redirector.

Perform the following procedure to enable debug traces for Cisco Web Dialer.

**Procedure**

**Step 1**
From the navigation drop-down list box of the Cisco Unified Communications Manager application, choose Cisco Unified Serviceability and then click **Go**.

**Step 2**
Choose **Trace > Configuration**.

**Step 3**
From the Server drop-down list box, choose the server on which you want to enable traces for Cisco Web Dialer.

**Step 4**
From the Service drop-down list box, choose the **Cisco Web Dialer Web Service**.

**Step 5**
In the Trace Configuration window, change the trace settings according to your troubleshooting requirements. For more information on traces, see the **Cisco Unified Serviceability Administration Guide**.

**Step 6**
Click **Save**.

---

**Additional Information**

See the “Related Topics” section on page 17-14.

**Related Topics**

- Configuration Checklist for Cisco Web Dialer, page 17-1
- Introducing Cisco Web Dialer, page 17-2
- Redundancy, page 17-3
- System Requirements for Cisco Web Dialer, page 17-4
- Interactions and Restrictions, page 17-4
- Installing and Activating Cisco Web Dialer, page 17-5
- Configuring Cisco Web Dialer, page 17-6
- Service Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
• Application Dial Rule Configuration, Cisco Unified Communications Manager Administration Guide

Additional Cisco Documentation
• Cisco Unified Serviceability Administration Guide
• Cisco Unified Communications Manager Security Guide
• Cisco Unified Communications Manager Release 8.0—This suite of documents relates to the installation and configuration of Cisco Unified Communications Manager. See the Cisco Unified Communications Manager Documentation Guide for Release 8.5(1) for a list of documents on installing and configuring Cisco Unified Communications Manager 8.0.
• Cisco Unified IP Phones for Cisco Unified Communications Manager—This suite of documents relates to the installation and configuration of Cisco Unified IP Phones.
• Cisco Unified IP Phone User Guides for Cisco Unified Communications Manager—The Customizing Your Phone on the Web section of each User Guide describes how to use the Cisco Unified CM User Options windows. This section provides information on Cisco Web Dialer, so the user can make calls from the web by clicking a telephone number that is linked to the company directory.
Client Matter Codes and Forced Authorization Codes

Forced Authorization Codes (FAC) and Client Matter Codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

The CMC and FAC features require that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC and/or CMC for each route pattern.

This chapter contains information on the following topics:

- Configuration Checklist for Client Matter Codes and Forced Authorization Codes, page 18-2
- Introducing Client Matter Codes, page 18-2
- Introducing Forced Authorization Codes, page 18-3
- Interactions and Restrictions, page 18-4
- System Requirements, page 18-6
- Installation of CMC and FAC, page 18-6
- Configuring Client Matter Codes, page 18-7
- CMC Configuration Settings, page 18-7
- Enabling Client Matter Codes For Route Patterns, page 18-8
- Configuring Forced Authorization Codes, page 18-9
- FAC Configuration Settings, page 18-9
- Enabling Forced Authorization Codes for Route Patterns, page 18-10
- Providing Information to Users, page 18-11
- Using CDR Analysis and Reporting, page 18-6
- Related Topics, page 18-11
Forced Authorization Codes (FAC) and Client Matter Codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

Use Table 18-1 as a guide when you configure client matter codes and forced authorization codes. For more information on client matter codes and forced authorization codes, see the “Related Topics” section on page 18-11.

### Table 18-1  Cisco CMC and FAC Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Review feature limitations.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Design and document the system; for example, document a list of client matters that you want to track.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Insert the codes by using Cisco Unified Communications Manager Administration or by using Bulk Administration Tool (BAT).</td>
</tr>
<tr>
<td>Step 4</td>
<td>To enable FAC or CMC, add or update route patterns in Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Provide all necessary information, for example, codes, to users and explain how the features works.</td>
</tr>
</tbody>
</table>

#### Additional Information
See the “Related Topics” section on page 18-11.

### Introducing Client Matter Codes

To use the Client Matter Codes feature, users must enter a client matter code to reach certain dialed numbers. You enable or disable CMC through route patterns, and you can configure multiple client matter codes. When a user dials a number that is routed through a CMC-enabled route pattern, a tone
Introducing Forced Authorization Codes

When you enable FAC through route patterns in Cisco Unified Communications Manager Administration, users must enter an authorization code to reach the intended recipient of the call. When a user dials a number that is routed through a FAC-enabled route pattern, the system plays a tone that prompts for the authorization code.

In Cisco Unified Communications Manager Administration, you can configure various levels of authorization. If the user authorization code does not meet or exceed the level of authorization that is specified to route the dialed number, the user receives a reorder tone. If the authorization is accepted, the call occurs. The name of the authorization writes to call detail records (CDRs), so you can organize the information by using CDR Analysis and Reporting (CAR), which generates reports for accounting and billing.

You can use FAC for colleges, universities, or any business or organization when limiting access to specific classes of calls proves beneficial. Likewise, when you assign unique authorization codes, you can determine which users placed calls. For each user, you specify an authorization code, then enable FAC for relevant route patterns by selecting the appropriate check box and specifying the minimum
Interactions and Restrictions

You can implement CMC and FAC separately or together. For example, you may authorize users to place certain classes of calls, such as long distance calls, and also assign the class of calls to a specific client. If you implement CMC and FAC together as described in the previous example, the user dials a number, enters the user-specific authorization code when prompted to do so, and then enters the client matter code at the next prompt. CMC and FAC tones sound the same to the user, so the feature tells the user to enter the authorization code after the first tone and enter the CMC after the second tone.

Cisco Unified Communications Manager provides redundancy, which handles the normal processes that are in place for Cisco Unified Communications Manager.

The CMC and FAC features work with all Cisco Unified IP Phones running SCCP and MGCP-controlled analog gateways.

Before you implement CMC and FAC, review the following restrictions:

- Because the number of CMCs directly impacts the time required for Cisco Unified Communications Manager to start up, the number of CMCs should be limited to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires 1 hour to start up; a system with 1 million CMCs requires 4 hours to start up.
- After dialing the phone number, hearing-impaired users should wait 1 or 2 seconds before entering the authorization or client matter code.
- Calls that are forwarded to a FAC- or CMC-enabled route pattern fail because no user is present to enter the code. This limitation applies to call forwarding that is configured in Cisco Unified Communications Manager Administration or the Cisco Unified CM User Options pages. You can configure call forwarding, but all calls that are forwarded to a FAC- or CMC-enabled route pattern results in reorder. When a user presses the CFwdALL softkey and enters a number that has FAC or CMC enabled on the route pattern, the user receives reorder, and call forwarding fails.
You cannot prevent the configuration of call forwarding to a FAC- or CMC-enabled route pattern; forwarded calls that use these route patterns drop because no code is entered. To minimize call-processing interruptions, test the number before you configure call forwarding. To do this, dial the intended forwarding number; if you are prompted for a code, do not configure call forwarding for that number. Advise users of this practice to reduce the number of complaints that result from forwarded calls that do not reach the intended destination.

- Cisco does not localize FAC or CMC. The CMC and FAC features use the same default tone for any locale that is supported with Cisco Unified Communications Manager.

- The CMC and FAC features do not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Require Forced Authorization Code or the Require Client Matter Code check box on the Route Pattern Configuration window, the Allow Overlap Sending check box becomes disabled. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code and the Require Client Matter Code check boxes become disabled.

- The FAC and CMC tones play only on Cisco Unified IP Phones that are running SCCP, TAPI/JTAPI ports, and MGCP FXS ports.

- Because no method exists to play the FAC or CMC tone over a trunk, calls that originate from a SIP trunk, H323, or MGCP gateway fail if they encounter a route pattern that requires FAC or CMC.

- H.323 analog gateways do not support FAC or CMC because these gateways cannot play tones.

- Restrictions apply to CTI devices that support FAC and CMC. For more information, see the “Using FAC/CMC with CTI, JTAPI, and TAPI Applications” section on page 18-6.

- Cisco Web Dialer does not support FAC or CMC.

- Cisco IP Softphone cannot play tones; however, after a Cisco IP Softphone user dials a directory number, the user can use CMC and FAC by waiting 1 or 2 seconds before entering the code.

- If you do not append the FAC or CMC with #, the system waits for the T302 timer to extend the call.

- When you press the Redial softkey on the phone, you must enter the authorization code or CMC when the number that you dialed is routed through a FAC- or CMC-enabled route pattern. Cisco does not save the code that you entered for the previous call.

- You cannot configure authorization code or CMC for speed-dial buttons. You must enter the code when the system prompts you to do so.

**Additional Information**

See the “Related Topics” section on page 18-11.

### Using the Cisco Bulk Administration Tool

You can use Bulk Administration Tool (BAT) to insert, update, and delete CMC and FAC. For more information on how to perform these tasks, see the *Cisco Unified Communications Manager Bulk Administration Guide* that is compatible with this release of Cisco Unified Communications Manager.

**Additional Information**

See the “Related Topics” section on page 18-11.
Using CDR Analysis and Reporting

CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for authorization code names, authorization levels, and CMCs. For information on how to generate reports in CAR, see the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide.

Additional Information
See the “Related Topics” section on page 18-11.

Using FAC/CMC with CTI, JTAPI, and TAPI Applications

In most cases, Cisco Unified Communications Manager can alert a CTI, JTAPI, or TAPI application that the user must enter a code during a call. When a user places a call, creates an ad hoc conference, or performs a consult transfer through a FAC- or CMC-enabled route pattern, the user must enter a code after receiving the tone. When a user redirects or blind transfers a call through a FAC- or CMC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco Unified Communications Manager. If Cisco Unified Communications Manager receives the appropriate codes, the call connects to the intended party. If Cisco Unified Communications Manager does not receive the appropriate codes, Cisco Unified Communications Manager sends an error to the application that indicates which code is missing.

Cisco Unified Communications Manager does not support call forwarding through FAC- or CMC-enabled route patterns. For more information, see the “Interactions and Restrictions” section on page 18-4.

Additional Information
See the “Related Topics” section on page 18-11.

System Requirements

The minimum requirements for CMC and FAC specify that every server in the cluster must have Cisco Unified Communications Manager 5.0 or a later version.

The following Cisco Unified IP Phones (SCCP) support CMC and FAC:
- Cisco Unified IP Phones 6900
- Cisco Unified IP Phones 7900

Additional Information
See the “Related Topics” section on page 18-11.

Installation of CMC and FAC

The CMC and FAC features install automatically when you install Cisco Unified Communications Manager. To make these features work in your Cisco Unified Communications Manager network, you must perform the tasks that are described in the “Configuring Client Matter Codes” section on page 18-7.
Configuring Client Matter Codes

After you obtain the list of CMCs that you plan to use, you add those codes to the database and enable the CMC feature for route patterns.

This section contains the information on the following topics:

- CMC Configuration Settings, page 18-7
- Enabling Client Matter Codes For Route Patterns, page 18-8

Tip

Before you configure client matter codes, review the “Configuration Checklist for Client Matter Codes and Forced Authorization Codes” section on page 18-2.

CMC Configuration Settings

In Cisco Unified Communications Manager Administration, use the Call Routing > Client Matter Codes menu path to configure client matter codes.

Client matter codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients by forcing the user to enter a code to specify that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes.

Tips About Configuring Client Matter Codes

You enter CMCs in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). If you use BAT, the BAT comma separated values (CSV) file provides a record of CMCs and client names. After you configure CMC, make sure that you update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

After you add all CMCs, see the “Enabling Client Matter Codes For Route Patterns” section on page 18-8.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Use Table 18-1 as a guide when you configure client matter codes. For more information on client matter codes and forced authorization codes, see the “Related Topics” section on page 18-11.

Additional Information

See the “Related Topics” section on page 18-11.
Table 18-2 describes the client matter codes configuration settings. Use this table in conjunction with the “Configuring Client Matter Codes” section on page 18-7.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Matter Code</td>
<td>Enter a unique code of no more than 16 digits that the user will enter when placing a call. The CMC displays in the CDRs for calls that use this code.</td>
</tr>
<tr>
<td>Description</td>
<td>This optional field associates a client code with a client. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), angle brackets (&lt;&gt;), or either type of brackets ([ ] {}).</td>
</tr>
</tbody>
</table>

Additional Information
See the “Related Topics” section on page 18-11.

Enabling Client Matter Codes For Route Patterns

Perform the following steps to enable CMCs on route patterns:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose Call Routing > Route/Hunt > Route Pattern.

Step 2 Perform one of the following tasks:
  • To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in “Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide.
  • To add a new route pattern, see “Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide.

Step 3 In the Route Pattern Configuration window, check the Require Client Matter Code check box.

Step 4 Perform one of the following tasks:
  • If you updated the route pattern, click Save.
  • If you added a new route pattern, click Save.

Step 5 Repeat Step 2 through Step 4 for all route patterns that require a client matter code.

Step 6 After you complete the route pattern configuration, see the “Providing Information to Users” section on page 18-11.

Additional Information
See the “Related Topics” section on page 18-11.
Configuring Forced Authorization Codes

This section contains information on the following topics:

- FAC Configuration Settings, page 18-9
- Enabling Forced Authorization Codes for Route Patterns, page 18-10

Tip

Before you configure forced authorization codes, review the “Configuration Checklist for Client Matter Codes and Forced Authorization Codes” section on page 18-2.

After you design your FAC implementation, you enter authorization codes either in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). Consider using BAT for large batches of authorization codes; the comma separated values (CSV) file in BAT serves as a blueprint for authorization codes, corresponding names, and corresponding levels.

Note

For future reference, make sure that you update your dial plan documents or keep a printout of the CSV file with your dial plan documents.

FAC Configuration Settings

In Cisco Unified Communications Manager Administration, use the Call Routing > Forced Authorization Codes menu path to configure forced authorization codes.

Forced Authorization Codes (FAC) allow you to manage call access and accounting by regulating the types of calls that certain users can place. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

Tips About Configuring Forced Authorization Codes

After you add all authorization codes, see the “Enabling Forced Authorization Codes for Route Patterns” section on page 18-10.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the “Navigating the Cisco Unified Communications Manager Administration Application” section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Use Table 18-1 as a guide when you configure forced authorization codes. For more information on forced authorization codes, see the “Related Topics” section on page 18-11.
Table 18-3 describes the FAC configuration settings. Use this table in conjunction with the “Configuring Forced Authorization Codes” section on page 18-9.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Code Name</td>
<td>Enter a unique name that is no more than 50 characters. This name ties the authorization code to a specific user or group of users; this name displays in the CDRs for calls that use this code.</td>
</tr>
<tr>
<td>Authorization Code</td>
<td>Enter a unique authorization code that is no more than 16 digits. The user enters this code when the user places a call through a FAC-enabled route pattern.</td>
</tr>
<tr>
<td>Authorization Level</td>
<td>Enter a three-digit authorization level that exists in the range of 0 to 255; the default equals 0. The level that you assign to the authorization code determines whether the user can route calls through FAC-enabled route patterns. To successfully route a call, the user authorization level must equal or be greater than the authorization level that is specified for the route pattern for the call.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 18-11.

Enabling Forced Authorization Codes for Route Patterns

Perform the following steps to enable FACs for route patterns:

Procedure

Step 1

In Cisco Unified Communications Manager Administration, choose Call Routing > Route/Hunt > Route Pattern.

Step 2

Perform one of the following tasks:

- To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in “Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide.
- To add a new route pattern, see “Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide.

Step 3

In the Route Pattern Configuration window, check the Require Forced Authorization Code check box.

Step 4

Click Save.

Tip

Even if you do not check the Require Forced Authorization Code check box, you can specify the authorization level because the database stores the number that you specify.

Step 5

Repeat Step 2 through Step 4 for all route patterns that require an authorization code.
Step 6  
After you complete the route pattern configuration, see the “Providing Information to Users” section on page 18-11.

Additional Information
See the “Related Topics” section on page 18-11.

Providing Information to Users

After you configure the feature(s), communicate the following information to your users:

- Inform users about restrictions that are described in “Interactions and Restrictions” section on page 18-4.
- Provide users with all necessary information to use the features; for example, authorization code, authorization level, client matter code, and so on. Inform users that dialing a number produces a tone that prompts for the codes.
- For FAC, the system attributes calls that are placed with the user authorization code to the user or the user department. Advise users to memorize the authorization code or to keep a record of it in a secure location.
- Advise users of the types of calls that users can place; before a user notifies a phone administrator about a problem, users should hang up and retry the dialed number and code.
- Inform users that they can start entering the code before the tone completes.
- To immediately route the call after the user enters the code, the users can press # on the phone; otherwise, the call occurs after the interdigit timer (T302) expires; that is, after 15 seconds by default.
- The phone plays a reorder tone when the user enters an invalid code. If users misdial the code, the user must hang up and try the call again. If the reorder tone persists, users should notify the phone or system administrator that a problem may exist with the code.

Additional Information
See the “Related Topics” section on page 18-11.

Related Topics

- Route Pattern Configuration, *Cisco Unified Communications Manager Administration Guide*
- Understanding Route Plans, *Cisco Unified Communications Manager System Guide*
- Interactions and Restrictions, page 18-4
- System Requirements, page 18-6
- Providing Information to Users, page 18-11

Client Matter Codes

- Configuration Checklist for Client Matter Codes and Forced Authorization Codes, page 18-2
- Introducing Client Matter Codes, page 18-2
Chapter 18      Client Matter Codes and Forced Authorization Codes

- CMC Configuration Settings, page 18-7
- Enabling Client Matter Codes For Route Patterns, page 18-8

Forced Authorization Codes
- Configuration Checklist for Client Matter Codes and Forced Authorization Codes, page 18-2
- Introducing Forced Authorization Codes, page 18-3
- FAC Configuration Settings, page 18-9
- Enabling Forced Authorization Codes for Route Patterns, page 18-10

Additional Cisco Documentation
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide
- Cisco Unified IP Phone Administration Guide
- Cisco Unified IP Phone Phone Guide
Custom Phone Rings

This chapter describes how you can customize the phone ring types that are available at your site by creating your own PCM files and editing the Ringlist.xml file.

This chapter covers the following topics:

- Introducing Custom Phone Rings, page 19-1
- Customizing and Modifying Configuration Files, page 19-2
- Ringlist.xml File Format Requirements, page 19-2
- PCM File Requirements for Custom Ring Types, page 19-3
- Configuring a Custom Phone Ring, page 19-3
- Related Topics, page 19-3

Introducing Custom Phone Rings

Cisco Unified IP Phones ship with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco Unified Communications Manager also provides a default set of additional phone ring sounds that are implemented in software as pulse code modulation (PCM) files. The PCM files, along with an XML file (named Ringlist.xml) that describes the ring list options that are available at your site, exist in the TFTP directory on each Cisco Unified Communications Manager server.

You can get a copy of the Ringlist.xml file from the system using the following admin cli “file” commands:

- admin:file
  - file list*
  - file view*
  - file search*
  - file get*
  - file dump*
  - file tail*
  - file delete*
Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and/or add customized files to the TFTP directory in Cisco Unified Communications Operating System Administration, from the TFTP Server File Upload page. See the Cisco Unified Communications Operating System Administration Guide for information on how to upload files to the TFTP folder on a Cisco Unified Communications Manager server.

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will display on the Ring Type menu on a Cisco Unified IP Phone for that ring.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRinglist>
    <Ring>
        <DisplayName/>
        <FileName/>
    </Ring>
</CiscoIPPhoneRinglist>
```

The following characteristics apply to the definition names:

- **DisplayName** defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu on a Cisco Unified IP Phone for that ring.
- **FileName** specifies the name of the PCM file for the custom ring to associate with **DisplayName**.

**Tip**

The **DisplayName** and **FileName** fields must not exceed 25 characters.

The following example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRinglist>
    <Ring>
        <DisplayName>Analog Synth 1</DisplayName>
        <FileName>Analog1.raw</FileName>
    </Ring>
    <Ring>
        <DisplayName>Analog Synth 2</DisplayName>
        <FileName>Analog2.raw</FileName>
    </Ring>
</CiscoIPPhoneRinglist>
```

**Tip**

You must include the required **DisplayName** and **FileName** for each phone ring type. The Ringlist.xml file can include up to 50 ring types.
PCM File Requirements for Custom Ring Types

The PCM files for the rings must meet the following requirements for proper playback on Cisco Unified IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- mu-law compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring evenly divisible by 240
- Ring starts and ends at the zero crossing.
- To create PCM files for custom phone rings, you can use any standard audio editing packages that support these file format requirements.

Configuring a Custom Phone Ring

The following procedure applies to creating custom phone rings for only the Cisco Unified IP Phones 7940, 7960, and 7970.

Procedure

- **Step 1** Create a PCM file for each custom ring (one ring per file). Ensure that the PCM files comply with the format guidelines that are listed in the “PCM File Requirements for Custom Ring Types” section on page 19-3.
- **Step 2** Use an ASCII editor to edit the Ringlist.xml file. See the “Ringlist.xml File Format Requirements” section on page 19-2 for information on how to format this file, along with a sample Ringlist.xml file.
- **Step 3** Save your modifications and close the Ringlist.xml file.
- **Step 4** Upload the Ringlist.xml file by using the Cisco Unified Communications Operating System. See the Cisco Unified Communications Operating System Administration Guide.
- **Step 5** To cache the new Ringlist.xml file, stop and start the TFTP service by using Cisco Unified Serviceability or disable and reenable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter (located in the Advanced Service Parameters).

Additional Information

See the “Related Topics” section on page 19-3.

Related Topics

- [Cisco TFTP](#), [Cisco Unified Communications Manager System Guide](#)
- [Service Parameter Configuration](#), [Cisco Unified Communications Manager Administration Guide](#)
Additional Cisco Documentation

- Cisco Unified IP Phone Administration documentation for Cisco Unified IP Phones 7940, 7960, and 7970
- *Cisco Unified Communications Operating System Administration Guide*
Device Mobility

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

You can configure device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility within a cluster, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

This chapter includes information on the following topics:

- Configuration Checklist for Device Mobility, page 20-2
- Introducing Device Mobility, page 20-3
- Understanding How Device Mobility Works, page 20-3
  - Device Mobility Operations Summary, page 20-5
  - Device Mobility Groups Operations Summary, page 20-6
  - Network Considerations, page 20-7
- Interactions and Restrictions, page 20-8
- System Requirements, page 20-9
- Installing Device Mobility, page 20-10
- Configuring Device Mobility, page 20-10
- Viewing Roaming Device Pool Parameters, page 20-21
- Related Topics, page 20-21
Configuration Checklist for Device Mobility

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

You can configure device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

For more information on device mobility, see the “Introducing Device Mobility” section on page 20-3 and the “Related Topics” section on page 20-21.

Table 20-1 shows the steps for configuring device mobility.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| **Step 1**          | Review the related device mobility documentation. (Tip: For information on dial plan design considerations, see the Cisco Unified Communications Solution Reference Network Design (SRND), which provides information on building class of service if you use device mobility.) | Cisco Unified Communications Solution Reference Network Design (SRND)  
Device Mobility, page 20-1 |
| **Step 2**          | Enable the device mobility mode in the Service Parameter Configuration or Phone Configuration window. *(System > Service Parameters* (choose Cisco CallManager service) or *Device > Phone)* | Viewing Roaming Device Pool Parameters, page 20-21 |
| **Step 3**          | Configure physical locations. *(System > Physical Location)* | Configuring a Physical Location, page 20-13  
Physical Location Configuration Settings, page 20-14 |
| **Step 4**          | Configure device mobility groups. *(System > Device Mobility > Device Mobility Groups)* | Configuring a Device Mobility Group, page 20-16  
Device Mobility Group Configuration Settings, page 20-17 |
| **Step 5**          | Configure subnets and assign one or more device pools to a subnet in the Device Mobility Info Configuration window. *(System > Device Mobility > Device Mobility Info)* | Configuring Device Mobility Information, page 20-19  
Device Mobility Info Configuration Settings, page 20-19 |
Introducing Device Mobility

With Cisco Unified Communications Manager, a site or a physical location gets identified by using various settings, such as locations, regions, calling search spaces, and media resources. Cisco Unified IP Phones that reside at a particular site get statically configured with these settings, and Cisco Unified Communications Manager uses these settings for proper call establishment, call routing, media resource selection, and so forth. However, when phones get moved from the home location to a remote location, these phones retain the home settings that are statically configured on the phones. Cisco Unified Communications Manager uses these home settings for the phones that are located at the remote site, which may cause problems with call routing, codec selection, media resource selection, and other call processing functions.

You can configure device mobility, which allows Cisco Unified Communications Manager to determine whether the phone is at its home location or at a roaming location. Cisco Unified Communications Manager uses the device IP subnets to determine the exact location of the phone. By enabling device mobility within a cluster, mobile users can roam from one site to another and acquire the site-specific settings. Cisco Unified Communications Manager then uses these dynamically allocated settings for call routing, codec section, media resource selection, and so forth.

The dynamically reconfigured location settings ensure that voice quality and allocation of resources are appropriate for the new phone location:

- When a mobile user moves to another location, call admission control (CAC) can ensure video and audio quality with the appropriate bandwidth allocations.
- When a mobile user makes a PSTN call, the phone can access the local gateway instead of the home gateway.
- When a mobile user calls the home location, Cisco Unified Communications Manager can assign the appropriate codec for the region.

Understanding How Device Mobility Works

When a phone device has mobility mode enabled, Cisco Unified Communications Manager uses the IP address of the registering device to find the proper location settings. The system compares the physical location that is configured in the device pool for the IP subnet and for the device to determine when a phone is away from its home location.
For example, phone A in Richardson with an IP address 10.81.17.9 registers with Cisco Unified Communications Manager. This IP address maps to subnet 10.81.16.0/16. Cisco Unified Communications Manager checks the device pool settings for the device and the subnet in the database. The physical location setting for the device pool in the phone record matches the physical location setting for the device pool in the subnet. The system considers the phone to be in its home location and uses the configuration settings in the phone record.

If phone A moves to Boulder, the phone queries the local DHCP server and gets an IP address of 130.5.5.25, which maps to subnet 130.5.5.0/8. Cisco Unified Communications Manager compares the physical location for the device pool in the phone record to the device pool location setting that is configured for the subnet. The system determines that the device is roaming because the physical locations do not match. Cisco Unified Communications Manager overwrites the phone record configuration settings with configuration settings for the subnet, downloads the settings in a new configuration file, and resets the device. The phone reregisters with the settings from the roaming device pool.

Note

The phone must have a dynamic IP address to use device mobility. If a phone with a static IP address roams, Cisco Unified Communications Manager uses the configuration settings from its home location.

For roaming devices, Cisco Unified Communications Manager overwrites the following device pool parameters with the device pool settings for the subnet:

- Date/Time Group
- Region
- Location
- Network Locale
- SRST Reference
- Connection Monitor Duration
- Physical Location
- Device Mobility Group
- Media Resource Group List

When networks span geographic locations outside the United States, you can configure device mobility groups to allow phone users to use their configured dial plan no matter where they roam. When a device is roaming but remains in the same device mobility group, Cisco Unified Communications Manager also overwrites the following device pool parameters:

- AAR Group
- AAR Calling Search Space
- Device Calling Search Space

When the phone returns to its home location, the system disassociates the roaming device pool, downloads the configuration settings for home location, and resets the device. The device registers with the home location configuration settings.

See these topics for more specific details about the device mobility operations in different scenarios:

- Device Mobility Operations Summary
- Device Mobility Groups Operations Summary
- Device Mobility Operations Summary, page 20-5
Cisco Unified Communications Manager always uses the Communications Manager Group setting from the phone record. The device always registers to its home location Cisco Unified Communications Manager server even when roaming. When a phone is roaming, only network location settings such as bandwidth allocation, media resource allocation, region configuration, and AAR group get changed.

**Device Mobility Operations Summary**

This section describes how Cisco Unified Communications Manager manages phone registration and assignment of parameters for device mobility.

Following initialization, the device mobility feature operates according to the following process:

1. A phone device record gets created for an IP phone that is provisioned to be mobile, and the phone gets assigned to a device pool. The phone registers with Cisco Unified Communications Manager, and an IP address gets assigned as part of the registration process.

2. Cisco Unified Communications Manager compares the IP address of the device to the subnets that are configured for device mobility in the Device Mobility Info Configuration window. The best match uses the largest number of bits in the IP subnet mask (longest match rule). For example, the IP address 9.9.8.2 matches the subnet 9.9.8.0/24 rather than the subnet 9.9.0.0/16.

3. If the device pool in the phone record matches the device pool in the matching subnet, the system considers the phone to be in its home location, and the phone retains the parameters of its home device pool.

4. If the device pool in the phone record does not match the device pools in the matching subnet, the system considers the phone to be roaming. Table 20-2 describes possible scenarios for device mobility and the system responses.

<table>
<thead>
<tr>
<th>Table 20-2 Device Mobility Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scenario</strong></td>
</tr>
<tr>
<td>The physical location setting in the phone device pool matches the physical location setting in a device pool that is associated with the matching subnet. Note Although the phone may have moved from one subnet to another, the physical location and associated services have not changed.</td>
</tr>
<tr>
<td>The matching subnet has a single device pool that is assigned to it; the subnet device pool differs from the home location device pool, and the physical locations differ.</td>
</tr>
<tr>
<td>The physical locations differ, and the matching subnet has multiple device pools assigned to it.</td>
</tr>
</tbody>
</table>
Understanding How Device Mobility Works

Device Mobility Groups Operations Summary

You can use device mobility groups to determine when a device moves to another location within a geographic entity, so a user can use its own dial plan. For example, you can configure a device mobility group for the United States and another group for the United Kingdom. If a phone moves into a different mobility group (such as from the United States to the United Kingdom), Cisco Unified Communications Manager uses the Calling Search Space, AAR Group and AAR CSS from the phone record, and not from the roaming location.

If the device moves to another location with same mobility group (for example, Richardson, USA, to Boulder, USA), the CSS information will get taken from the roaming device pool settings. With this approach, if the user is dialing PSTN destinations, the user will reach the local gateway.

Table 20-3 describes the device pool parameters that the system uses for various scenarios.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Parameters Used</th>
</tr>
</thead>
</table>
| A roaming device moves to another location in the same device mobility group. | Roaming Device Pool: yes  
Location: Roaming device pool setting  
Region: Roaming device pool setting  
Media Resources Group List: Roaming device pool setting  
Device CSS: Roaming device pool setting (Device Mobility CSS)  
AAR Group: Roaming device pool setting  
AAR CSS: Roaming device pool setting |
Understanding How Device Mobility Works

Network Considerations

The device mobility structure accommodates different network configurations.

For efficient device mobility design, divide the network into device mobility groups (optional), physical locations, and subnets. The number and levels of groups in the hierarchy depend on the size and complexity of the organization.

- Device mobility groups represent the top-level geographic entities in your network. The device mobility group setting determines whether the device is moved within the same geographical entity, primarily to allow users to keep their own dial plans. The device mobility group defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg). For example, if you want a roaming device to access the local gateway for PSTN calls, be sure that the device mobility group for the home location device pool and roaming location device pool are the same.

  Device mobility groups could represent countries, regions, states or provinces, cities, or other entities. An enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities. The system does not require defining device mobility groups to use the device mobility feature.

- Physical location, the next level in the hierarchy, identifies a geographic location for device pool parameters that are location-based, such as date/time, region, and so on. Cisco Unified Communications Manager uses the geographic location to determine which network resources to assign to a phone. If a user moves away from the home location, the system ensures that the phone user uses local media resources and the correct bandwidth for the call.

  For example, a Music on Hold (MOH) server may serve a specific office or campus within the enterprise. When a device roams to another office or campus and reregisters with Cisco Unified Communications Manager, having the device served by the MOH server at the roaming location represents best practice.

  By defining the physical location according to availability of services such as MOH, you can assure efficient and cost-effective reassignment of services as devices move from one physical location to another. Depending upon the network structure and allocation of services, you can define physical locations based upon city, enterprise campus, or building.
Ideally, your network configuration places each network in one physical location, so a network can be mapped to a single physical location.

- A subnet may include all the devices at a geographical location, within the same building, or on the same LAN. You can configure one or more device pools, including device mobility group and physical location, for a subnet.
- Location identifies the CAC for a centralized call-processing system. You configure a location for a phone and a device pool. See the Call Admission Control chapter in the Cisco Unified Communications Manager System Guide for more information.

For information on dial plan design considerations, see the Cisco Unified Communications Solution Reference Network Design (SRND), which provides information on building class of service if you use device mobility.

### Interactions and Restrictions

#### Calling Party Normalization

Calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without the need to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone. For information on how calling party normalization works with device mobility, see the “Interactions and Restrictions” section on page 8-10 in the “Calling Party Normalization” chapter.

#### IP Address

The Device Mobility feature depends on the IPv4 address of the device that registers with Cisco Unified Communications Manager.

- The phone must have a dynamic IPv4 address to use device mobility.
- If the device is assigned an IP address by using NAT/PAT, the IP address that is provided during registration may not match the actual IP address of the device.

#### IPv6 and Device Mobility

Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

#### Roaming

When a device is roaming in the same device mobility group, Cisco Unified Communications Manager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the CFA CSS is set to None, and the CFA CSS Activation Policy is set to With Activating Device/Line CSS, then:

- The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.
- If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS get used as the CFA CSS.
- If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.
For more information about configuration options for Call Forward All, see the Directory Number Configuration chapter in the Cisco Unified Communications Manager Administration Guide and the Understanding Directory Numbers chapter in the Cisco Unified Communications Manager System Guide.

System Requirements

Device Mobility requires the following software components:

- Cisco CallManager service running on at least one server in the cluster
- Cisco Database Layer Monitor service running on the same server as the Cisco CallManager service
- Cisco TFTP service running on at least one server in the cluster
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones)

Any phone that is running either SCCP or SIP and that can be configured in Cisco Unified Communications Manager Administration supports device mobility, including:

- Cisco Unified IP Phone 6900 series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 series
- Cisco Unified IP Phone 8900 series
- Cisco Unified IP Phone 9900 series
- Computer Telephony Integration (CTI) Ports
- Cisco IP Communicator

For more information about IP Phones and the device mobility feature, see the user guides at the following sites:


Devices That Support Device Mobility

Use the Cisco Unified Reporting application to generate a complete list of devices that support device mobility. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application:

   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.
2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all devices that support device mobility, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Mobility

   The List Features pane displays a list of all devices that support the mobility feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

For additional information about the Cisco Unified Reporting application, see the **Cisco Unified Reporting Administration Guide**, which you can find at this URL:


---

### Installing Device Mobility

Device mobility automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure device mobility settings in Cisco Unified Communications Manager Administration to enable the feature.

**Note**
Existing device pools automatically migrate to the new device pool and common profile structure as part of the upgrade to Cisco Unified Communications Manager Release 6.0 or later.

### Configuring Device Mobility

For successful configuration of the device mobility feature, review the network design considerations, review the steps in the configuration checklist, perform the configuration requirements, and activate the Cisco CallManager service, if it is not already activated.

For an overview of device mobility parameter settings, see the following sections:
- **Configuration Tips for Device Mobility**, page 20-11
- **Enabling Device Mobility**, page 20-12
- **Configuring Device Pools for Device Mobility**, page 20-21

#### Physical Locations
- **Finding a Physical Location**, page 20-12
- **Configuring a Physical Location**, page 20-13
- **Physical Location Configuration Settings**, page 20-14
- **Deleting a Physical Location**, page 20-15

#### Device Mobility Groups
- **Finding Device Mobility Groups**, page 20-15
Configuration Tips for Device Mobility

Consider the following information when you configure device mobility in Cisco Unified Communications Manager Administration:

- When the Device Mobility Mode is set to Default in the Phone Configuration window, the Device Mobility Mode service parameter determines whether the device is enabled for the device mobility feature.
- Cisco Unified Communications Manager uses the longest match rule to match IP addresses and subnets, meaning the best match uses the largest number of bits in the IP subnet mask. For example, the IP address 9.9.8.2 matches the subnet 9.9.8.0/24 rather than the subnet 9.9.0.0/16.
- If no device mobility information entries match the device IP address, the device uses the home location device pool settings.
- You assign the device pool to the phone device in the Phone Configuration window; you assign device pools to subnets in the Device Mobility Info Configuration window.
- You can assign one or more device pools to a subnet address. Cisco Unified Communications Manager assigns device pools for the same subnet to roaming devices in round-robin fashion; for example, roaming device 1 gets assigned the first device pool in the list, and roaming device 2 gets assigned the second device pool in the list. This process allows you to load share when you expect a large number of phones to roam into an area, such as a meeting in the head office that employees from all branch locations will attend.
- Although physical location does not represent a required setting in the Device Pool Configuration window, you must define a physical location for a device pool to use the device mobility feature. Be sure to configure physical location for the home location device pool and for the roaming device pool.
- After the device mobility structure is in place, you can turn device mobility on for IP phones that support device mobility.

Additional Information

See the “Related Topics” section on page 20-21.
Enabling Device Mobility

This section describes the procedure to enable the device mobility feature in the Service Parameter or Phone Configuration window.

Consider the following information when enabling the device mobility feature:

- When device mobility mode is enabled or disabled for the cluster, the cluster setting applies to all phones in the cluster that support device mobility. At installation, the default setting for the Device Mobility Mode service parameter specifies Off, which means that device mobility is disabled.
- When device mobility mode is enabled or disabled in the Phone Configuration window, the Device Mobility Mode phone settings take precedence over the service parameter setting.
- When the phone setting for Device Mobility Mode equals Default, Cisco Unified Communications Manager uses the service parameter setting for the device.

Procedure

Step 1 To enable the Device Mobility service parameter, perform the following tasks:

a. Choose System > Service Parameters in Cisco Unified Communications Manager Administration.

b. From the Server drop-down list box, select the server that is running the Cisco CallManager service.

c. From the Service drop-down list box, select the Cisco CallManager service. The Service Parameters Configuration window displays.

d. To enable the Device Mobility Mode service parameter, choose On.

Step 2 To configure the Device Mobility Mode setting for a specific phone, perform the following tasks:

a. Choose Device > Phone in Cisco Unified Communications Manager Administration.

b. Click Find to display the device pools list, or use the search results from an active query.

c. Choose a device from the phone list that displays in the Find and List Phones window. The Phone Configuration window displays.

d. In the Device Mobility Mode drop-down list box, choose On to enable device mobility, choose Off to disable device mobility, or choose Default, which ensures that the phone uses the configuration from the Device Mobility Mode service parameter.

Finding a Physical Location

Because you may have several physical locations in your network, Cisco Unified Communications Manager lets you locate specific physical locations on the basis of specific criteria. Use the following procedure to locate physical locations.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your physical location search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your physical location search preferences until you modify your search or close the browser.
Chapter 20  Device Mobility

Configuring Device Mobility

Procedure

Step 1  Choose System > Physical Location.
   The Find and List Physical Locations window displays. Records from an active (prior) query may also display in the window.

Step 2  To find all records in the database, ensure the dialog box is empty; go to Step 3.
   To filter or search records
   • From the first drop-down list box, select a search parameter.
   • From the second drop-down list box, select a search pattern.
   • Specify the appropriate search text, if applicable.

   Note  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.
   All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

   Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

   Note  To reverse the sort order, click the up or down arrow, if available, in the list header.
   The window displays the item that you choose.

Additional Information
   See the “Related Topics” section on page 20-21.

Configuring a Physical Location

To add a physical location for a device pool, use the following procedure.

Procedure

Step 1  Choose System > Physical Location.
   The Find and List Physical Locations window displays.
Step 2  Perform one of the following tasks:

- To copy an existing physical location, locate the appropriate physical location as described in the “Finding a Physical Location” section on page 20-12, click the Copy button next to the physical location that you want to copy, and continue with Step 3.

- To add a new physical location, click the Add New button and continue with Step 3.

- To update an existing physical location, locate the appropriate physical location as described in the “Finding a Physical Location” section on page 20-12 and continue with Step 3.

Step 3  Enter the appropriate settings as described in Table 20-5.

Step 4  To save the physical location information in the database, click Save.

Additional Information

See the “Related Topics” section on page 20-21.

Physical Location Configuration Settings

A physical location, which is used with the device mobility feature, identifies a geographic location for device pool parameters that are location-based, such as date/time, region, and so on. Cisco Unified Communications Manager uses the geographic location to determine which network resources to assign to a phone. If a user moves away from the home location, the system ensures that the phone user uses local media resources and the correct bandwidth for the call.

For example, a Music on Hold (MOH) server may serve a specific office or campus within the enterprise. When a device roams to another office or campus and reregisters with Cisco Unified Communications Manager, having the device served by the MOH server at the roaming location represents best practice.

By defining the physical location according to availability of services such as MOH, you can assure efficient and cost-effective reassignment of services as devices move from one physical location to another. Depending upon the network structure and allocation of services, you can define physical locations based upon city, enterprise campus, or building.

Ideally, your network configuration places each network in one physical location, so a network can be mapped to a single physical location. Depending upon the network structure and allocation of services, you may define physical locations based upon a city, enterprise campus, or building.

Table 20-5 describes the physical location configuration settings. For related procedures, see the “Related Topics” section on page 20-21.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Location Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the physical location. The name can contain up to 50 alphanumeric characters with any combination of spaces, periods (.), hyphens (-), underscore characters (_).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter text describing the physical location. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
</tbody>
</table>
Deleting a Physical Location

If a physical location is currently used in a device pool, you cannot delete it. To delete the physical location, you can first find the associated device pools from the dependency record and disassociate them before deleting the physical location.

To delete a physical location, use the following procedure.

**Procedure**

**Step 1**
To locate the physical location that you want to delete, follow the procedure on “Finding a Physical Location” section on page 20-12.

**Step 2**
Check the check box next to the physical locations that you want to delete. To select all the physical locations in the window, check the check box in the matching records title bar.

**Step 3**
Click **Delete Selected**.

**Step 4**
To confirm your selection, click **OK**.

**Additional Information**
See the “Related Topics” section on page 20-21.

Finding Device Mobility Groups

Because you may have several device mobility groups in your network, Cisco Unified Communications Manager lets you locate specific device mobility groups on the basis of specific criteria. Use the following procedure to locate device mobility groups.

**Note**
During your work in a browser session, Cisco Unified Communications Manager Administration retains your device mobility group search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your device mobility group search preferences until you modify your search or close the browser.

**Procedure**

**Step 1**
Choose **System > Device Mobility > Device Mobility Group**.

The Find and List Device Mobility Groups window displays. Records from an active (prior) query may also display in the window.

**Step 2**
To find all records in the database, ensure the dialog box is empty; go to **Step 3**.

To filter or search records
- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

**Step 3**

Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Note**

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

**Step 4**

From the list of records that display, click the link for the record that you want to view.

**Note**

To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

**Additional Information**

See the “Related Topics” section on page 20-21.

## Configuring a Device Mobility Group

To configure a device mobility group, which supports the device mobility feature, use the following procedure.

**Procedure**

**Step 1**

Choose **System > Device Mobility > Device Mobility Group**.

The Find and List Device Mobility Groups window displays.

**Step 2**

Perform one of the following tasks:

- To copy an existing device mobility group, locate the appropriate device mobility group as described in the “Finding Device Mobility Groups” section on page 20-15, click the **Copy** button next to the device mobility group that you want to copy, and continue with **Step 3**.
- To add a new device mobility group, click the **Add New** button and continue with **Step 3**.
- To update an existing device mobility group, locate the appropriate device mobility group as described in the “Finding Device Mobility Groups” section on page 20-15 and continue with **Step 3**.

**Step 3**

Enter the appropriate fields as described in Table 20-5.

**Step 4**

Click **Save** to save the device mobility group information to the database.
Device Mobility Group Configuration Settings

Device mobility groups support the device mobility feature. Device mobility groups represent the highest level geographic entities in your network. Depending upon the network size and scope, your device mobility groups could represent countries, regions, states or provinces, cities, or other entities. For example, an enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities.

**Tip**
The device mobility group defines a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg).

Table 20-5 describes the device mobility group configuration settings. For related procedures, see the “Related Topics” section on page 20-21.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Mobility Group Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the device mobility group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the profile. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
</tbody>
</table>

Deleting a Device Mobility Group

If a device mobility group is currently used in a device pool, you cannot delete it. To delete the device mobility group, you must find the associated device pools from the dependency record, disassociate them, and then delete the device mobility group.

**Procedure**

1. **Step 1** To locate the device mobility group that you want to delete, follow the procedure in “Finding Device Mobility Groups” section on page 20-15.
2. **Step 2** Check the check box next to the device mobility groups that you want to delete. To select all the device mobility groups in the window, check the check box in the matching records title bar.
3. **Step 3** Click **Delete Selected**.
4. **Step 4** To confirm your selection, click **OK**.

**Additional Information**
See the “Related Topics” section on page 20-21.
Finding Device Mobility Info

Because you may have several device mobility info records in your network, Cisco Unified Communications Manager lets you locate specific device mobility information on the basis of specific criteria. Use the following procedure to locate device mobility information.

Note
During your work in a browser session, Cisco Unified Communications Manager Administration retains your device mobility info search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your device mobility info search preferences until you modify your search or close the browser.

Procedure

Step 1
Choose System > Device Mobility > Device Mobility Info.

The Find and List Device Mobility Infos window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3
Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note
You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4
From the list of records that display, click the link for the record that you want to view.

Note
To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Related Topics” section on page 20-21.
# Configuring Device Mobility Information

To add device mobility information, use the following procedure.

**Procedure**

**Step 1**  
Choose System > Device Mobility > Device Mobility Info.  
The Find and List Device Mobility Infos window displays.

**Step 2**  
Perform one of the following tasks:

- To copy an existing device mobility info, locate the appropriate device mobility info as described in the “Finding Device Mobility Info” section on page 20-18, click the **Copy** button next to the device mobility info that you want to copy, and continue with Step 3.
- To add a new device mobility info, click the **Add New** button and continue with Step 3.
- To update an existing device mobility info, locate the appropriate device mobility info as described in the “Finding Device Mobility Info” section on page 20-18 and continue with Step 3.

**Step 3**  
Enter the appropriate fields as described in Table 20-5.

**Step 4**  
To save the device mobility info information to the database, click **Save**.

**Additional Information**  
See the “Related Topics” section on page 20-21.

## Device Mobility Info Configuration Settings

The Device Mobility Info Configuration window specifies the subnets and device pools that are used for device mobility. When a phone registers with Cisco Unified Communications Manager, the system compares the IP address of the device to the subnets that are configured for device mobility in the Device Mobility Info Configuration window. The best match uses the largest number of bits in the IP subnet mask (longest match rule). For example, the IP address 9.9.8.2 matches the subnet 9.9.8.0/24 rather than the subnet 9.9.0.0/16.

If the device pool in the phone record matches the device pool in the matching subnet, the system considers the phone to be in its home location, and the phone retains the parameters of its home device pool.

If the device pool in the phone record does not match the device pools in the matching subnet, the system considers the phone to be roaming. Table 20-2 describes possible scenarios for device mobility and the system responses.

Table 20-5 describes the device mobility info configuration settings. For related procedures, see the “Related Topics” section on page 20-21.

### Table 20-5  Device Mobility Info Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Mobility Info Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the device mobility info record.</td>
</tr>
</tbody>
</table>
Deleting a Device Mobility Info

If you delete a device mobility info that is currently used by a device, Cisco Unified Communications Manager reapplies the appropriate device mobility rules according to the descriptions in the Device Mobility chapter.

To delete a device mobility info record, use the following procedure.

**Procedure**

1. **Step 1** To locate the device mobility info that you want to delete, follow the procedure in the “Finding Device Mobility Info” section on page 20-18.
2. **Step 2** Check the check box next to the device mobility record that you want to delete. To select all the records in the window, check the check box in the matching records title bar.
3. **Step 3** Click Delete Selected.
4. **Step 4** To confirm your selection, click OK.

**Additional Information**

See the “Related Topics” section on page 20-21.
Configuring Device Pools for Device Mobility

The roaming sensitive settings in the Device Pool Configuration window override the device-level settings when the device roams within or outside a device mobility group. The settings, which include Date/time Group, Region, Media Resource Group List, Location, Network Locale, SRST Reference, Physical Location, Device Mobility Group, and so on, provide call admission control and voice codec selection. Additionally, these settings update the media resource group list (MRGL), so appropriate remote media resources get used for music on hold, conferencing, transcoding, and so on. The roaming sensitive settings also update the Survivable Remote Site Telephony (SRST) gateway. Mobile users register to a different SRST gateway while roaming. This registration may affect the dialing behavior when the roaming phones are in SRST mode.

The device mobility related parameters in the Device Pool Configuration window override the device-level settings only when the device is roaming within a device mobility group. The device mobility related settings affect the dial plan because the calling search space dictates the patterns that can be dialed or the devices that can be reached.

See the “Device Pool Configuration” chapter in the Cisco Unified Communications Manager Administration Guide to configure device pool parameters.

Viewing Roaming Device Pool Parameters

When the phone has device mobility mode enabled, you can view the roaming device pool settings by clicking View Current Device Mobility Settings next to the Device Mobility Mode field in the Phone Configuration window. If the device is not roaming, the home location settings display.

Related Topics

- Configuration Checklist for Device Mobility, page 20-2
- Introducing Device Mobility, page 20-3
- Understanding How Device Mobility Works, page 20-3
- Device Mobility Operations Summary, page 20-5
- Device Mobility Groups Operations Summary, page 20-6
- Network Considerations, page 20-7
- Interactions and Restrictions, page 20-8
- System Requirements, page 20-9
- Installing Device Mobility, page 20-10
- Configuring Device Mobility, page 20-10
- Viewing Roaming Device Pool Parameters, page 20-21
- Calling Party Normalization, page 8-1
- Internet Protocol Version 6 (IPv6), page 29-1
- Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Common Device Configuration, Cisco Unified Communications Manager Administration Guide
Related Topics

- Location Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Survivable Remote Site Telephony Configuration, Cisco Unified Communications Manager Administration Guide
- Automated Alternate Routing Group Configuration, Cisco Unified Communications Manager Administration Guide
- Date/Time Group Configuration, Cisco Unified Communications Manager Administration Guide
- Region Configuration, Cisco Unified Communications Manager Administration Guide
- Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide
- Media Resource Group Configuration, Cisco Unified Communications Manager Administration Guide
- Call Admission Control, Cisco Unified Communications Manager System Guide
- System-Level Configuration Settings, Cisco Unified Communications Manager System Guide
- Cisco TFTP, Cisco Unified Communications Manager System Guide

Additional Cisco Documentation

- Cisco Unified Communications Solution Reference Network Design (SRND)
- Cisco Unified Serviceability Administration Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
Do Not Disturb

The Do Not Disturb (DND) feature provides the following options:

- **Call Reject**—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.
- **Ringer Off**—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call.

Users can configure DND directly from their Cisco Unified IP Phone or from the Cisco Unified CM User Options.

This chapter provides the following information about Do Not Disturb:

- Configuration Checklist for Do Not Disturb, page 21-1
- Introducing Do Not Disturb, page 21-2
- Overview of Do Not Disturb Architecture, page 21-3
- System Requirements for Do Not Disturb, page 21-3
- Interactions and Restrictions, page 21-5
- Installing and Activating Do Not Disturb, page 21-7
- Configuring Do Not Disturb, page 21-7
- How to Use Do Not Disturb, page 21-11
- Troubleshooting Do Not Disturb, page 21-16
- Related Topics, page 21-18

Configuration Checklist for Do Not Disturb

The Do Not Disturb (DND) feature provides the following options:

- **Call Reject**—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.
- **Ringer Off**—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call.
When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls or calls with Multi-Level Precedence & Preemption (MLPP), will ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

Table 21-1 provides a checklist to configure the Do Not Disturb feature. For more information on the Do Not Disturb feature, see the “Introducing Do Not Disturb” section on page 21-2 and the “Related Topics” section on page 21-18.

### Table 21-1  Do Not Disturb Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure DND service parameters.</td>
<td>Setting the Do Not Disturb Service Parameters, page 21-8</td>
</tr>
<tr>
<td><strong>Step 2</strong> Configure DND softkeys.</td>
<td>Configuring DND Softkeys, page 21-8</td>
</tr>
<tr>
<td><strong>Step 3</strong> Configure DND feature button.</td>
<td>Configuring a DND Button, page 21-9</td>
</tr>
<tr>
<td><strong>Step 4</strong> Configure device-based DND parameters.</td>
<td>Configuring Device Parameters for DND, page 21-9</td>
</tr>
<tr>
<td><strong>Step 5</strong> Configure phone profile settings.</td>
<td>Adding DND to Common Phone Profiles, page 21-11</td>
</tr>
</tbody>
</table>

### Introducing Do Not Disturb

When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls or calls with Multi-Level Precedence & Preemption (MLPP), will ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

The user can enable and disable DND by any of the following methods:
- Softkey
- Feature button
- Cisco Unified CM User Options windows

You can also enable and disable DND on a per-phone basis in Cisco Unified Communications Manager Administration.

When you enable DND, the Cisco Unified IP Phone displays the message **Do Not Disturb is active**. when DND is active. Some Cisco Unified IP Phones display DND status icons. For more information about Cisco Unified IP Phones and the DND feature, see the user guides for that IP phone.

### Incoming Call Alert Settings

DND incoming call alert settings determine how the incoming call alert gets presented to the user when DND Ringer Off or DND Call Reject is enabled. The following list gives the available options:
- **None**—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device.
- **Disable**—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device.
• **Beep Only**—For an incoming call, this option causes the phone to play a beep tone only.
• **Flash Only**—For an incoming call, this option causes the phone to display a flash alert.

You can configure DND Incoming Call Alert on a per-device basis and also configure it on the Common Phone Profile window for group settings. If you do not set up the configuration at the device level, the Common Phone Profile settings get used.

### Overview of Do Not Disturb Architecture

This section provides an overview of DND architecture for both SIP and SCCP devices and includes the following topics:

- **DND Status Notification for SIP Devices, page 21-3**
- **DND Status Notification for SCCP Devices, page 21-3**

### DND Status Notification for SIP Devices

Cisco Unified Communications Manager supports Do Not Disturb that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from a SIP device to Cisco Unified Communications Manager by using the SIP PUBLISH method (RFC3909). A DND status change gets signaled from a Cisco Unified Communications Manager to a SIP device by using a dndupdate Remote-cc REFER request. Cisco Unified Communications Manager can also publish the Do Not Disturb status for a device, along with the busy and idle status for the device.

### DND Status Notification for SCCP Devices

Cisco Skinny Client Control Protocol (SCCP) supports Do Not Disturb requests that an SCCP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from an SCCP device to Cisco Unified Communications Manager by using SCCP messaging.

### System Requirements for Do Not Disturb

The following sections provide software and hardware requirement for Do Not Disturb:

- **Software Requirements, page 21-3**
- **Hardware Requirements, page 21-4**

### Software Requirements

To operate, the Do Not Disturb feature requires the following software components:

- Cisco Unified Communications Manager Release 6.0(1) or later
Hardware Requirements

The following Cisco Unified IP Phones support the Do Not Disturb feature:

- Cisco Unified IP Phone 6900 series (except 6901 and 6911)
- Cisco Unified IP Phone 7900 series
- Cisco Unified IP Phone 8900 series
- Cisco Unified IP Phone 9900 series

Note

Cisco Unified IP Phones 7940 and 7960 that are running SIP use their own backwards-compatible implementation of Do Not Disturb, which you configure on the SIP Profile window.

For more information about Cisco Unified IP Phones and the DND feature, see the phone user guides at the following sites:


Devices That Support Do Not Disturb

Use the Cisco Unified Reporting application to generate a complete list of devices that support Do Not Disturb. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File > Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all devices that support DND, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Do Not Disturb

The List Features pane displays a list of all devices that support the DND. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.
Interactions and Restrictions

See the following sections for information on interactions and restrictions:

- Interactions, page 21-5
- Restrictions, page 21-7

Interactions

The following sections describe how the Do Not Disturb feature interacts with Cisco Unified Communications Manager applications and call processing:

- Call Forward All, page 21-5
- Park Reversion, page 21-5
- Pickup, page 21-6
- Hold Reversion and Intercom, page 21-6
- MLPP and CER, page 21-6
- Callback, page 21-6
- Pickup Notification, page 21-6
- Hunt List, page 21-6
- Extension Mobility, page 21-7

Call Forward All

On Cisco Unified IP Phones, the message that indicates that the Do Not Disturb (DND) feature is active takes priority over the message that indicates that the user has new voicemail messages, which allows the user to know when DND is active. However, the message that indicates that the Call Forward All feature is active has a higher priority than DND.

Park Reversion

For locally parked calls, Park Reversion overrides DND (both options). If Phone A has DND turned on and parked a call, the park reversion to Phone A will occur normally and will ring Phone A.

For remotely parked calls, DND overrides Park Reversion:

- If Phone A activates DND Ringer Off and shares a line with Phone A-prime, when Phone A-prime parks the call, park reversion on Phone A will not ring and will honor the DND settings.
- If Phone A activates DND Call Reject, the park reversion call will not be presented to Phone A.
Pickup

For a locally placed Pickup request, Pickup overrides DND (both options). If Phone A has DND turned on and has initiated any type of Pickup, the Pickup call would be presented normally, and it will ring Phone A.

For a remotely placed Pickup request, DND overrides Pickup.

- If Phone A (with DND Ringer Off activated) shares a line with Phone A-prime, when Phone A-prime initiates Pickup, the Pickup call to Phone A will not ring and will honor DND settings.
- If Phone A is in DND Call Reject mode, the Pickup call will not be presented to Phone A.

Hold Reversion and Intercom

Hold reversion and intercom override DND (both options), and the call gets presented normally.

MLPP and CER

MLPP (phones that are running SCCP) and CER calls override DND (both options). MLPP and CER calls get presented normally, and the phone will ring.

Callback

For the originating side, callback overrides DND. When the activating device is on DND mode (both options), the callback notification (both audio and visual) will still be presented to the user.

For the terminating side, DND overrides callback:

- When the terminating side is on DND Ringer Off, the Callback Available screen will be sent after the terminating side goes off hook and on hook.
- When the terminating side is on DND Call Reject and is available (goes off hook and on hook), a new screen will be sent to the activating device as “<DirectoryNumber> has become available but is on DND-R” if the activating device is in same cluster. Callback available notification will be sent only after the terminating side disables DND Call Reject.

Pickup Notification

For the DND Ringer Off option, only visual notification gets presented to the device.

For the DND Call Reject option, no notification gets presented to the device.

Hunt List

If a device in a Hunt List has DND Ringer Off activated, the call will still presented to the user when a call gets made to that Hunt List. However, the DND Incoming Call Alert settings would still apply.

If a device in a Hunt List has DND Call Reject activated, any calls to that Hunt List will go to the next member and will not get sent to this device.
Extension Mobility

For extension mobility, the device profile settings include DND incoming call alert and DND status. When a user logs in and enables DND, the DND incoming call alert and DND status settings get saved, and these settings get used when the user logs in again.

Note

When a user who is logged in to extension mobility modifies the DND incoming call alert or DND status settings, this action does not affect the actual device settings.

Restrictions

Some restrictions apply to DND usage, depending on the phone or device type in use.

- The following phone models and devices that are running SCCP support only the DND Ringer Off option:
  - Cisco Unified IP Phone 7940
  - Cisco Unified IP Phone 7960
  - Cisco IP Communicator

Note

Cisco Unified IP Phones 7940 and 7960 that run SIP use their own implementation of Do Not Disturb, which is backward compatible.

- The following phone models and devices support only the DND Call Reject option:
  - Mobile devices (dual mode)
  - Remote Destination Profile
  - Cisco Unified Mobile Communicator

Installing and Activating Do Not Disturb

Do Not Disturb, a system feature, comes standard with Cisco Unified Communications Manager software. It does not require special installation.

Configuring Do Not Disturb

This section describes the procedures for configuring the Do Not Disturb feature:

- Setting the Do Not Disturb Service Parameters, page 21-8
- Configuring DND Softkeys, page 21-8
- Configuring a DND Button, page 21-9
- Configuring Device Parameters for DND, page 21-9
- Adding DND to Common Phone Profiles, page 21-11
Tip
Before you configure the Do Not Disturb feature, review the “Configuration Checklist for Do Not Disturb” section on page 21-1.

Setting the Do Not Disturb Service Parameters

Cisco Unified Communications Manager provides one systemwide service parameter for Do Not Disturb: BLF Status Depicts DND. This parameter determines whether DND status is considered in the Busy Lamp Field (BLF) status calculation, and you can set the parameter to True or False.

- When you specify True for BLF Status Depicts DND and DND is activated on the device, the BLF status indicator for the device or line appearance reflects the DND state.
- When you specify False for BLF Status Depicts DND and DND is activated on the device, the BLF status indicator for the device or line appearance reflects the actual device state.

When BLF Status Depicts DND is enabled or disabled for the cluster, the cluster setting applies to all phones in the cluster that support DND.

Note
To set this service parameter, navigate to System > Service Parameters and choose the Cisco CallManager service for the server that you want to configure. Specify the desired state for BLF Status Depicts DND in the Clusterwide Parameters (System - Presence) pane.

Configuring DND Softkeys

Default softkey templates do not make a DND softkey available. To add a DND softkey, navigate to Device > Device Settings > Softkey Template, add Do Not Disturb to a softkey template in the Softkey Template Configuration window, and associate the template to the device.

A DND softkey is available in the following states:

- Connected
- Connected Conference
- Connected Transfer
- Off Hook
- Off Hook with Feature
- On Hold
- Remote In Use
- On Hook
- Ring In
- Ring Out
- Digits After First
Configuring a DND Button

To configure a DND button, navigate to Device > Device Settings > Phone Button Template and add Do Not Disturb in the Phone Button Template Configuration window.

Configuring Device Parameters for DND

To configure DND on a particular Cisco Unified IP Phone, navigate to Device > Phone and choose the phone that you want to configure. In the Do Not Disturb pane on the Phone Configuration window, configure the parameters that are shown in Table 21-2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Disturb</td>
<td>Check this check box to enable Do Not Disturb on the phone.</td>
</tr>
<tr>
<td>DND Option</td>
<td>When you enable DND on the phone, this parameter allows you to specify how</td>
</tr>
<tr>
<td></td>
<td>the DND features handle incoming calls:</td>
</tr>
<tr>
<td></td>
<td>• Call Reject—This option specifies that no incoming call information gets</td>
</tr>
<tr>
<td></td>
<td>presented to the user. Depending on how you configure the DND Incoming</td>
</tr>
<tr>
<td></td>
<td>Call Alert parameter, the phone may play a beep or display a flash</td>
</tr>
<tr>
<td></td>
<td>notification of the call.</td>
</tr>
<tr>
<td></td>
<td>• Ringer Off—This option turns off the ringer, but incoming call information</td>
</tr>
<tr>
<td></td>
<td>gets presented to the device, so that the user can accept the call.</td>
</tr>
<tr>
<td></td>
<td>• Use Common Phone Profile Setting—This option specifies that the DND</td>
</tr>
<tr>
<td></td>
<td>Option setting from the Common Phone Profile window will get used for</td>
</tr>
<tr>
<td></td>
<td>this device.</td>
</tr>
</tbody>
</table>

Note

For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.
### Table 21-2 DND Device Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| DND Incoming Call Alert | When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options:  
  - **None**—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device.  
  - **Disable**—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device.  
  - **Beep Only**—For an incoming call, this option causes the phone to play a beep tone only.  
  - **Flash Only**—For an incoming call, this option causes the phone to display a flash alert. |
Adding DND to Common Phone Profiles

To add DND to a common phone profile, navigate to Device > Device Settings > Common Phone Profile and choose the phone profile that you want to modify. In the Common Phone Profile Configuration window, configure the DND parameters that are shown in Table 21-3.

Table 21-3 Common Phone Profile DND Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DND Option</td>
<td>When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Call Reject</strong>—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ringer Off</strong>—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call.</td>
</tr>
<tr>
<td>Note</td>
<td>For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.</td>
</tr>
<tr>
<td>DND Incoming Call Alert</td>
<td>When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Beep Only</strong>—For an incoming call, this option causes the phone to play a beep tone only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Flash Only</strong>—For an incoming call, this option causes the phone to display a flash alert.</td>
</tr>
</tbody>
</table>

How to Use Do Not Disturb

This section provides instructions for using Do Not Disturb, as well as usage examples for different Do Not Disturb call scenarios.

- **Using the Do Not Disturb Feature, page 21-12**
- **Do Not Disturb Usage Examples, page 21-12**
Using the Do Not Disturb Feature

You can activate Do Not Disturb using any of the following methods:

- Softkey
- Feature button
- Cisco Unified CM User Options

After you activate DND, the phone status line displays **Do not disturb is active**, the DND line button icon becomes an empty circle, and the light turns amber.

When you activate DND, you can still receive incoming call notifications on the phone as specified by the incoming call alert settings in Cisco Unified Communications Manager administration, but the phone will not ring, except for high-priority calls (such as Cisco Emergency Responder and MLPP calls).

Also, if you enable DND while the phone is ringing, the phone stops ringing.

Do Not Disturb Usage Examples

This section provides several examples of how calls get presented to phones with the Do Not Disturb feature enabled for both the DND Ringer Off option and the DND Call Reject option.

- DND Ringer Off Option, page 21-12
- DND Call Reject Option, page 21-15

DND Ringer Off Option

The following examples use the DND Ringer Off option.

**Normal Priority Call with DND Ringer Off Enabled on a Nonshared Line**

*Figure 21-1* shows the steps that are associated with DND when you place a normal-priority call to a phone with DND Ringer Off enabled on a nonshared line:

1. Phone B activates DND. Phone B displays **Do Not Disturb is active**.
2. Phone A dials phone B.
3. Phone B beeps, and phone A receives ringback tone.
How to Use Do Not Disturb

**Figure 21-1 Normal Priority Call with DND Ringer Off Enabled on a Nonshared Line**

Phone A calls Phone B

Phone B is on DND Ringer Off with the DND Incoming Call Alert Setting as Beep Only

Cisco Unified Communications Manager extends the call to Phone B. Phone B will only get a Beep to indicate an incoming call.

Normal Priority Call with DND Ringer Off Enabled on a Shared Line

Figure 21-2 shows the steps that are associated with DND when you place a normal-priority call to a phone with DND Ringer Off enabled on a shared line:

1. Phone B activates DND. Phone B displays Do Not Disturb is active.
2. Phone A dials a shared line on phone B.
3. Phone B beeps, and phone B’, which shares the line, rings normally.
4. Phone A receives ringback tone.
**Figure 21-2 Normal Priority Call with DND Ringer Off Enabled on a Shared Line**

Phone A calls Phone B

Phone B' rings normally

Phone B

Cisco Unified Communications Manager

Cisco Unified Communications Manager extends the call to Phone B. Phone B will only get a Beep to indicate an incoming call.

Phone B is on DND Ringer Off with the DND Incoming Call Alert Setting as Beep Only.

**High Priority Call with DND Ringer Off Enabled on a Shared Line**

Figure 21-3 shows the steps that are associated with DND when you place a high-priority call to a phone with DND Ringer Off enabled on a shared line:

1. Phone B activates DND. Phone B displays **Do Not Disturb is active**.
2. Phone A dials a shared line on phone B.
3. Phone B beeps, and phone B’, which shares the line, rings normally.
4. Phone A receives ringback tone.
5. Phone B answers and parks the call.
6. Park reversion occurs, and phone B rings normally.
Chapter 21      Do Not Disturb

How to Use Do Not Disturb

Figure 21-3  High Priority Call with DND Ringer Off Enabled on a Shared Line

Normal Call with DND and Call Forward No Answer Enabled on a Nonshared Line

The following steps show the call flow for a call that you make to a phone with both DND and Call Forward No Answer active:

1. Phone B configures Call Forward No Answer to forward calls to Phone C.
2. Phone B activates DND.
3. Phone A calls Phone B.
4. Phone B beeps and does not answer the call.
5. The call gets forwarded to phone C, which rings normally.

DND Call Reject Option

The following examples use the DND Call Reject option.

Normal Priority Call with DND Call Reject Enabled on a Nonshared Line

The following steps show the call flow for a call with Call Reject enabled on a nonshared line:

1. Phone B activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A calls Phone B.
3. Cisco Unified Communications Manager rejects the call with the reason User Busy.
4. Phone B gets a beep tone only.

Normal Priority Call with DND Call Reject Enabled on a Shared Line

The following steps show the call flow for a call with Call Reject enabled on a shared line:

1. Phone B activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A calls Phone B.
3. Cisco Unified Communications Manager rejects the call with the reason User Busy.
4. Phone B gets a beep tone only.
5. Phone B-prime, which is not on DND, rings normally.

High-Priority Call with DND Call Reject Enabled on a Shared Line
The following steps show the call flow for a high-priority call with DND Call Reject enabled on a shared line:
1. Phone A activates DND Call Reject with a DND Incoming Call Alert setting of Beep Only.
2. Phone A calls Phone B.
3. Cisco Unified Communications Manager extends the call to Phone B.
4. Phone B answers the call.
5. Phone A parks the call.
6. Phone A-prime, which is not on DND, rings normally.
7. Park Reversion occurs, and Phone A rings normally.

Troubleshooting Do Not Disturb
The section provides troubleshooting information for Cisco Unified IP Phones (SCCP and SIP).
- Basic DND Troubleshooting, page 21-16
- Troubleshooting Phones That Are Running SIP, page 21-17
- Troubleshooting Phones That Are Running SCCP, page 21-17
- Troubleshooting DND Errors, page 21-17

Basic DND Troubleshooting
If DND does not operate as expected, determine whether the settings maintained by the SCCP station code are the same as what the user thinks they are, as shown in the following examples.

Verify DND status by toggling DND
If you toggle DND status using a softkey or a feature button, you can see the new status in the LmFeatureInd message that is sent to line control. (The new status implies the old status was the opposite.) You can then toggle back.

The LmFeatureInd SDL trace gives the following three fields:
- **feature**: A value of 4 indicates DND.
- **featureState**: A value of 0 indicates **on**; a value of 1 indicates **off**.
- **dndOption**: A value of 0 indicates unknown; a value of 1 indicates ringer-off, and a value of 2 indicates call-reject.

Verify all DND settings by resetting the phone
If you reset the phone, all of the DND settings will be printed in the detailed SDI traces, for example:

```
StationD: (xxxxxxx) DND settings from TSP:
status=a, option=b, ringSetting=d
```
where

- \( a \) equals 0 (DND off) or 1 (DND on)
- \( b \) equals 1 (DND ringer-off option, 1 indicates ringer-off)
- \( d \) equals 1 (disable ringer), 2 (flash only), or 5 (beep only)

**Troubleshooting Phones That Are Running SIP**

Use the following information to troubleshoot phones that are running SIP:

- debugs: sip-dnd, sip-messages, dnd-settings
- show: config, dnd-settings
- Sniffer traces

**Troubleshooting Phones That Are Running SCCP**

Use the following information to troubleshoot phones that are running SCCP:

- debug: jvm all info
- Sniffer traces

**Troubleshooting DND Errors**

Table 21-4 shows symptoms and actions for DND troubleshooting.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Actions</th>
</tr>
</thead>
</table>
| DND feature key does not display | • Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above.  
                                              • Verify the button template for this phone has the DND feature key.  
                                              • Capture a sniffer trace and verify that the phone gets the correct button template.  
                                              • Verify that the phone is running firmware 8.3(1) and above. |
| DND softkey does not display    | • Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above.  
                                              • Verify the softkey template for this phone has DND.  
                                              • Capture a sniffer trace and verify that the phone gets the correct softkey template.  
                                              • Verify that the phone is running firmware 8.3(1) and above. |
Table 21-4  DND Troubleshooting Symptoms and Actions (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLF speed dial does not show DND status</td>
<td>• Check the Cisco Unified Communications Manager version and ensure that it is 6.0 or above.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the BLF DND is set to enabled in Enterprise parameters.</td>
</tr>
<tr>
<td></td>
<td>• Capture a sniffer trace and verify that the phone gets the correct NotificationMessage.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the phone is running firmware 8.3(1) and above.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuration Checklist for Do Not Disturb, page 21-1
- Introducing Do Not Disturb, page 21-2
- Overview of Do Not Disturb Architecture, page 21-3
- System Requirements for Do Not Disturb, page 21-3
- Interactions and Restrictions, page 21-5
- Installing and Activating Do Not Disturb, page 21-7
- Configuring Do Not Disturb, page 21-7
- How to Use Do Not Disturb, page 21-11
- Troubleshooting Do Not Disturb, page 21-16
Cisco Unified Communications Manager 8.0(2) (or higher) supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied. The following examples show how external call control can work:

- **Best Quality Voice Routing**—The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.
- **Least Cost Routing**—The adjunct route server is configured with carrier contract information such as Lata and Inter-Lata rate plans, trunking costs, and burst utilization costs to ensure calls are routed over the most cost effective links.
- **Ethical Wall**—The adjunct route server is configured with corporate policies that determine reachability; for example, Is user 1 allowed to call user 2?. When Cisco Unified Communications Manager issues a route request, the route server sends a response that indicates whether the call should be allowed, denied, or redirected to another party.


This chapter contains information on the following topics:

- **Configuration Checklist for External Call Control**, page 22-2
- **Introducing External Call Control for Cisco Unified Communications Manager**, page 22-5
- **System Requirements for External Call Control**, page 22-10
- **Interactions and Restrictions**, page 22-10
- **Installing and Activating External Call Control**, page 22-13
- **Configuring External Call Control**, page 22-13
Configuration Checklist for External Call Control

Cisco Unified Communications Manager, Release 8.0(2) (or higher), supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied. The following examples show how external call control can work:

- **Best Quality Voice Routing**—The adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.
- **Least Cost Routing**—The adjunct route server is configured with carrier contract information such as Lata and Inter-Lata rate plans, trunking costs, and burst utilization costs to ensure calls are routed over the most cost effective links.
- **Ethical Wall**—The adjunct route server is configured with corporate policies that determine reachability; for example, Is user 1 allowed to call user 2?. When Cisco Unified Communications Manager issues a route request, the route server sends a response that indicates whether the call should be allowed, denied, or redirected to another party.
Table 22-1 provides a checklist for configuring external call control in your network. For more information on how external call control works, see the “Introducing External Call Control for Cisco Unified Communications Manager” section on page 22-5 and the “Interactions and Restrictions” section on page 22-10.

**Table 22-1 External Call Control Configuration Checklist**

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Set up the Cisco Unified Routing Rules Interface so that the route server can direct Cisco Unified Communications Manager on how to handle calls.</td>
<td>Cisco Unified Communications Manager XML Developers Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong> Configure a calling search space that Cisco Unified Communications Manager uses when the route server sends a divert obligation to Cisco Unified Communications Manager. (Call Routing &gt; Class of Control &gt; Calling Search Space) You assign this calling search space to the external call control profile when you configure the profile.</td>
<td>Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 3</strong> Configure the external call control profile(s). (Call Routing &gt; External Call Control Profile)</td>
<td>External Call Control Profile Configuration Settings, page 22-15 Finding Configuration Records for External Call Control Profiles, page 22-19 Configuring an External Call Control Profile, page 22-20</td>
</tr>
<tr>
<td><strong>Step 4</strong> For the translation patterns that you want to use with external call control, assign an external call control profile to the pattern. (Call Routing &gt; Translation Pattern)</td>
<td>Assigning the External Call Control Profile to the Translation Pattern, page 22-21</td>
</tr>
<tr>
<td><strong>Step 5</strong> If the route server uses https, import the certificate for the route server into the trusted store on the Cisco Unified Communications Manager server. (In Cisco Unified Communications Operating System, choose Security &gt; Certificate Management.) You must perform this task on each node in the cluster that can send routing queries to the route server.</td>
<td>External Call Control Profile Configuration Settings, page 22-15</td>
</tr>
<tr>
<td><strong>Step 6</strong> If the route server uses https, export the Cisco Unified Communications Manager self-signed certificate to the route server. (In Cisco Unified Communications Operating System, choose Security &gt; Certificate Management.) You must perform this task for each node in the cluster that can send routing queries to the route server.</td>
<td>Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export, page 22-22</td>
</tr>
</tbody>
</table>
## Table 22-1 External Call Control Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Chaperone Support for Routing Rules, page 22-9</strong></td>
</tr>
</tbody>
</table>
| If your routing rules from the route server state that a chaperone must monitor and/or record a call, configure chaperone functionality in Cisco Unified Communications Manager Administration.  
  - For phones where you want to enable recording, set the Built-in-Bridge to **On** in the Phone Configuration window.  
  - Create a recording profile. Choose **Device > Device Settings > Recording Profile**, and create a Call Recording Profile for the phones that can record chaperoned conferences.  
  - Apply the recording profile to the line appearance.  
  - Add a SIP trunk to point to the recorder, and create a route pattern that points to the SIP Trunk.  
  - Configure the Play Recording Notification Tone to Observed Target and Play Recording Notification Tone to Observed Connected Target service parameters.  
  - Assign the Standard Chaperone Phone softkey template to the phone that the chaperone uses.  
  - Make sure that the chaperone phone does not have shared lines or multiple directory numbers/lines configured for it. Configure only one directory number for the chaperone phone. (Call Routing > Directory Number or Device > Phone if the phone is already configured)  
  - For the directory number on the chaperone phone, choose **Device Invoked Call Recording Enabled** from the Recording Option drop-down list box. (Call Routing > Directory Number or Device > Phone if the phone is already configured)  
  - For the directory number on the chaperone phone, enter 2 for the Maximum Number of Calls setting, and enter 1 for the Busy Trigger setting. (Call Routing > Directory Number or Device > Phone if the phone is already configured)  
  - For Cisco Unified IP Phones that support the Record softkey, make sure that the Standard Chaperone Phone softkey template is configured so that only the conference, record, and end call softkeys display on the phone in a connected state.  
  - For Cisco Unified IP Phones that support the Record programmable line keys (PLK), configure the PLK in the Phone Button Template Configuration window.  
  - If you have more than one chaperone in your cluster, add the chaperone DN to the chaperone line group that you plan to assign to the chaperone hunt list. Adding the chaperone to the line group, which belongs to the hunt list, ensures that an available chaperone monitors the call. |
Introducing External Call Control for Cisco Unified Communications Manager

Cisco Unified Communications Manager, Release 8.0(2) (or higher), supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

Tip
Be aware that routing rules or business logic on the adjunct route server determine how the call is handled. If your configuration in Cisco Unified Communications Manager Administration conflicts with the routing rules, the routing rule gets used for the call.

In Cisco Unified Communications Manager Administration, you enable external call control on translation patterns by assigning a configured external call control profile to the translation pattern. The following example demonstrates how external call control works in your network:

1. Cisco Unified Communications Manager receives an incoming call, and the digit analysis engine in Cisco Unified Communications Manager selects the best matching translation pattern.

2. If you assigned a configured external call control profile to the translation pattern, Cisco Unified Communications Manager does not extend the call to the device. Instead, Cisco Unified Communications Manager sends a call-routing query by using XACML (eXtensible Access Control Markup Language) over http or https using the POST method to the route server.

   Cisco Unified Communications Manager may include the calling number, transformed calling number, called number or dialed digits, transformed called number, and the trigger point information (string for translation pattern) in the query.

3. Routing rules and business logic on the route server determine how to route the call. The route server sends a call routing directive to Cisco Unified Communications Manager, and Cisco Unified Communications Manager follows the directive to handle the call. When the route server responds to Cisco Unified Communications Manager, the route server sends a XACML directive that consists of a route decision and an obligation. The route decision may include the following values for the decision:
- Permit—Call is allowed.
- Deny—Call is denied.
- Indeterminate—No call routing rule is determined. (usually related to a configuration issue)
- Not applicable—No call routing rule matches the request.

The obligation, which contain instructions that are specifically customized for Cisco Unified Communications Manager, gets encoded in Call Instruction XML (CIXML). The obligation must be consistent with the route decision. If it is not consistent, Cisco Unified Communications Manager obeys the route decision. Additionally, the obligation may contain parameters, which provide a reason code or additional tasks that Cisco Unified Communications Manager must perform when handling the call. Table 22-2 describes the obligations and related parameters for the obligation.

<table>
<thead>
<tr>
<th>Obligation</th>
<th>Description</th>
<th>Parameters for Obligation</th>
</tr>
</thead>
</table>
| Reject     | The adjunct route server may issue a Reject obligation for a Permit or Deny decision. Cisco Unified Communications Manager rejects the call, and the caller receives a fast busy tone. If the route decision is Deny and no obligation gets sent, Cisco Unified Communications Manager treats the call as if a Reject obligation is issued. | The reject obligation may contain the following parameters:  
  • Announce—Cisco Unified Communications Manager plays a specified announcement, identified by [id], to the caller that indicates that the call is rejected.  
  • Reason—A string indicates why the call was rejected; the reason string is used for alarm and logging purposes. When the reason indicates that a route violation occurred, the alarm, CallAttemptBlockedByPolicy, gets raised for the event. |
| Continue   | The route decision must be Permit for the Continue obligation to be used. If the decision is Deny, then the obligation is ignored. Cisco Unified Communications Manager routes the call to the current destination; that is, Cisco Unified Communications Manager manipulates the digits as expected and routes the call. Modified calling/called numbers in the continue obligation override the result of the transformation on the translation pattern and may change the destination of the call. If the adjunct route server issues a Permit decision and no obligation gets sent, Cisco Unified Communications Manager treats the call as if a Continue obligation is issued. | The continue obligation may contain the following parameters, which are optional:  
  • Greeting—Cisco Unified Communications Manager plays an announcement, identified by [id], to the caller before connecting the caller to the called party.  
  • Modify—The adjunct route server overwrites the calling and called party transformation that is configured for the translation pattern. Cisco Unified Communications Manager changes the calling or called number(s) to the numbers that are provided in the directive. If the number is not included in the directive, the configuration for the route pattern or translation pattern applies. |
Cisco Unified Communications Manager Connections to the Adjunct Route Server(s)

Cisco Unified Communications Manager maintains persistent connections to the adjunct route server to reduce delays with call setup. Each node in a Cisco Unified Communications Manager cluster may establish multiple connections to the adjunct route server for parallel/simultaneous queries at a high call rate. Cisco Unified Communications Manager manages a thread pool for the persistent connections, which is determined by the configuration for the following service parameters:

- **External Call Control Initial Connection Count To PDP**—This parameter specifies the minimum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests.

- **External Call Control Maximum Connection Count To PDP**—This parameter specifies the maximum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests.

For more information on these and other external call control service parameters, see the “Service Parameters for External Call Control” section on page 22-13.
External Call Control Profiles

In Cisco Unified Communications Manager Administration, you enable external call control by assigning a configured external call control profile to the translation pattern. The translation pattern is the trigger point for external call control; that is, if the translation pattern has an external call control profile assigned to it, when the called number on the call matches the translation pattern, Cisco Unified Communications Manager immediately sends a call-routing query to an adjunct route server, and the adjunct route server directs Cisco Unified Communications Manager on how to handle the call.

The external call control profile provides the URIs for a primary and redundant adjunct route server (called the web service in the GUI), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

In the external call control profiles that you configure in Cisco Unified Communications Manager Administration, you must provide the URI(s) for the adjunct route server(s) that provides the route decisions and obligations to the Cisco Unified Communications Manager. If you want to do so, you can configure one URI, known as the primary web service in Cisco Unified Communications Manager Administration, or you can configure primary and secondary URIs to create active and standby links to the adjunct route server(s). If you configure primary and secondary URIs, the route servers can load balance the call-routing queries in a round robin fashion. For the URIs, you can use http or https. If you specify https, Cisco Unified Communications Manager uses certificates to mutually authenticate via a TLS connection to the adjunct route server.

If you use https, Cisco Unified Communications Manager verifies that the certificate subject name matches the hostname of the adjunct route server. Additionally, Cisco Unified Communications Manager verifies whether the signature of the certificate is issued by a trusted CA or if the signature matches a self-signed, imported certificate in the trusted store.

To establish https connections, you must import certificates from each adjunct route server into the trusted store on each Cisco Unified Communications Manager node. Likewise, you must export a self-signed certificate from each Cisco Unified Communications Manager node and import it to the trusted store on each adjunct route server. For more information on these tasks, see the “External Call Control Profile Configuration Settings” section on page 22-15 and the “Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export” section on page 22-22.

If Cisco Unified Communications Manager must redirect a call because the adjunct route server issues a divert routing directive, the configuration for the Diversion Rerouting CSS gets used.

In the external call control profile, you can configure the time that Cisco Unified Communications Manager waits for a response from the adjunct route server. If the timer expires, Cisco Unified Communications Manager either allows or blocks the call, based on how you configured the Call Treatment on Failure setting in the external call control profile.
Chaperone Support for Routing Rules

If routing rules from the adjunct route server state that a chaperone must be present on a call, you must configure chaperone support in Cisco Unified Communications Manager Administration. In this case, the adjunct route server sends the following routing directive to Cisco Unified Communications Manager:

- Permit decision
- Divert obligation that contains reason = chaperone.

A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Cisco Unified Communications Manager provides the following capabilities to support chaperone functionality, as directed by the adjunct route server:

- Cisco Unified Communications Manager can redirect an incoming call to a chaperone or hunt group/list of chaperones.
- Cisco Unified Communications Manager can provide a chaperone with the ability to record a call. When the chaperone is connected to the caller or when the chaperoned conference is established, the Record softkey or PLK (depending on the phone model) becomes active on the phone so that the chaperone can invoke call recording. Call recording occurs for the current call only, and call recording stops when the current call ends. Messages that indicate the status of recording may display on the phone when the chaperone presses the recording softkey/PLK.

For a list of configuration tasks that you must perform in Cisco Unified Communications Manager Administration to set up chaperon support, see the “Configuration Checklist for External Call Control” section on page 22-2.

Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone. The following restrictions exist for chaperones:

- The chaperone cannot use the phone to put the conference call on hold.
- The chaperone cannot use the phone to add parties to a conference after the conference begins because the call must be put on hold for the chaperone to add parties.

After the chaperone creates a conference, the conference softkey gets disabled on the phone; that is, if the phone uses the conference softkey.

Be aware that the other parties on the conference may be able to add additional parties to the conference. The configuration for the Advanced Ad Hoc Conference Enabled service parameter, which supports the Cisco CallManager service, determines whether other parties can add participants to the conference. If the service parameter is set to True, other parties can add participants to the conference.

- The chaperone cannot use the phone to transfer the conference call to another party.
- When the chaperone leaves the conference, the entire conference drops.
- If the chaperone starts recording before making a consultative call to the party that should join the conference, Cisco Unified Communications Manager suspends recording while the chaperone makes the consultative call; recording resumes after the conference is established.
Announcement Support for Routing Rules

Routing rules on the adjunct route server may require that Cisco Unified Communications Manager play an announcement for the call; for example, an announcement that states that the call is rejected or an announcement that issues a greeting to the caller before connecting the caller to the called party. When you install Cisco Unified Communications Manager, Cisco-provided announcements and tones install, and the Find and Lists Announcements window in Cisco Unified Communications Manager Administration displays these announcements and tones, which can be used for external call control. (Media Resources > Announcements) All announcements that display in the window support external call control, but the obligation that the adjunct route server issues determines which announcement Cisco Unified Communications Manager plays; for example, the obligation from the adjunct route server indicates that Cisco Unified Communications Manager must reject the call and play the Custom_05006 announcement.

Tip

If you want to use customized announcements, not the Cisco-provided announcements, you can upload the customized announcements in the Announcements Configuration window.

For More Information

Announcement Configuration, Cisco Unified Communications Manager Administration Guide

System Requirements for External Call Control

The following system requirements exist for external call control:

- Cisco Unified Communications Manager 8.0(2) (or higher)
- Cisco Unified Routing Rules XML Interface, which provides the route decisions and obligation for the calls

Interactions and Restrictions

Annunciator

If your routing rules require that an announcement get played for calls, upload or customize the standard announcements in the Announcements window; that is, if you do not want to use the Cisco-provided announcements. (Media Resources > Announcements)

In you upload customized announcements, configure annunciator so that you can use the announcements. (Media Resources > Annunciator)

Best Call Quality Routing for Cisco Unified Communications Manager Calls

If you want to do so, you can set up routing rules on the adjunct route server that determine which gateway should be used for a call when voice quality is a consideration; for example, gateway A provides the best voice quality, so it gets used for the call. In this case, the adjunct route server monitors network link availability, bandwidth usage, latency, jitter, and MOS scores to ensure calls are routed through voice gateways that deliver the best voice quality to all call participants.
Call Detail Records

External call control functionality can display in call detail records; for example, the call detail record can indicate whether the adjunct route server permitted or rejected the call. In addition, the call detail record can indicate whether Cisco Unified Communications Manager blocked or allowed calls when Cisco Unified Communications Manager did not receive a decision from the adjunct route server. For more information on call detail records and external call control, see the Cisco Unified Communications Manager Call Detail Records Administration Guide.

Call Forward

External call control intercepts calls at the translation pattern level, while call forward intercepts calls at the directory number level. External call control has higher priority; that is, for calls where call forward is invoked, Cisco Unified Communications Manager sends a routing query to the adjunct route server if the translation pattern has an external call control profile assigned to it. Call forwarding gets triggered only when the adjunct route server sends a Permit decision with a Continue obligation to the Cisco Unified Communications Manager.

Be aware that the call diversion hop count service parameter that supports external call control and the call forward call hop count service parameter that supports call forwarding are independent; that is, they work separately.

Call Pickup

When Cisco Unified Communications Manager recognizes that a phone user is trying to pick up a call by using the call pickup feature, external call control does not get invoked; that is, Cisco Unified Communications Manager does not send a routing query to the adjunct route server for that portion of the call.

Chaperones

A chaperone is a designated phone user who can announce company policies to the call, monitor the call, and record the call, if required. Chaperone restrictions exist so that the parties that are involved in the call cannot converse without the presence of the chaperone. For chaperone restrictions, see the “Chaperone Support for Routing Rules” section on page 22-9.

Cisco Unified Mobility

Cisco Unified Communications Manager honors the route decision from the adjunct route server for the following Cisco Unified Mobility features:

- Mobile Connect
- Mobile Voice Access
- Enterprise Feature Access
- Dial-via-Office Reverse Callback
- Dial-via-Office Forward

Tip

To invoke Mobile Voice Access or Enterprise Feature Access, the end user must dial a feature directory number that is configured in Cisco Unified Communications Manager Administration. When the Cisco Unified Communications Manager receives the call, Cisco Unified Communications Manager does not invoke external call control because the called number, in this case, is the feature DN. After the call is anchored, the Cisco Unified Communications Manager asks for user authentication, and the user enters the number for the target party. When Cisco Unified Communications Manager tries to extend the call to the target party, external call control gets invoked, and Cisco Unified Communications Manager sends a call routing query to the adjunct route server to determine how to handle the call.
Cisco Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features:

- Cell pickup
- Desk pickup
- Session handoff

**Cisco Unified Serviceability**

Alarm definitions for external call control display in Cisco Unified Serviceability under the Cisco CallManager alarm catalog. For information on the alarm definitions, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

**Conferences**

When a phone user creates a conference, external call control may get invoked for the primary call and consultative call.

**Directory Numbers**

When you configure directory numbers as 4- or 5-digit extensions (enterprise extensions), you need to configure 2 translation patterns if on-net dialing supports 4 or 5 digits. One translation pattern supports globalizing the calling/called numbers, and a second translation pattern supports localizing the calling/called numbers. Assign external call control profile on the translation pattern that is used for globalizing the calling/called numbers.

**Do Not Disturb**

By default, the DND setting for the user takes effect when the user rule on the adjunct route server indicates that the adjunct route server send a continue obligation. For example, if the adjunct route server sends a continue obligation, and the user has DND-R enabled, Cisco Unified Communications Manager rejects the call.

**Emergency Call Handling (for example, 911 or 9.11)**

---

**Caution**

Cisco strongly recommends that you configure a very explicit set of patterns for emergency calls (for example, 911 or 9.911) so that the calls route to their proper destination (for example, to Cisco Emergency Responder or a gateway) without having to contact the route server for instructions on how to handle the call.

---

For example, if you configure your system so that all calls that originate from a group of phones use the external call control feature, all calls, including emergency calls, get routed to the route server. In this case, how the calls get handled depends on the rules configuration on the route server. If the route server does not issue a Permit directive (or if the route server does not have a rule or business logic for handling emergency calls), an emergency call may be denied (or there may be a delay in processing the call).
Real Time Monitoring Tool
For external call control, performance monitoring counters display under the External Call Control object and the Cisco CallManager object in RTMT. For information on these counters, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Transfer
When a phone user transfers a call, external call control may get invoked for both the primary call and consultative call. However, Cisco Unified Communications Manager cannot enforce any routing rules from the adjunct route server between the party that transfers and the target of the transfer.

Installing and Activating External Call Control
After you install Cisco Unified Communications Manager, your network can support external call control if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for External Call Control” section on page 22-2.

Configuring External Call Control
This section contains information on the following topics:

- Service Parameters for External Call Control, page 22-13
- External Call Control Profile Configuration Settings, page 22-15
- Finding Configuration Records for External Call Control Profiles, page 22-19
- Configuring an External Call Control Profile, page 22-20
- Assigning the External Call Control Profile to the Translation Pattern, page 22-21
- Deleting Configuration Records for External Call Control Profiles, page 22-21
- Importing the Adjunct Route Server Certificate, page 22-22
- Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export, page 22-22

Tip
Before you configure external call control, review the “Configuration Checklist for External Call Control” section on page 22-2.

Service Parameters for External Call Control

To access the service parameters that support the external call control feature, choose System > Service Parameters. Choose the server and the Cisco CallManager service. Then, locate the Clusterwide Parameters (Feature - External Call Control) pane. Table 22-3 describes the service parameters for the external call control feature. For additional information, you can click the question mark help in the Service Parameters window.
### Table 22-3  External Call Control Service Parameters

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Call Control Diversion Maximum Hop Count</td>
<td>This parameter specifies the maximum number of times the adjunct route server can issue a divert obligation for a single call. The default equals 12. The minimum value is 1, and the maximum value is 500.</td>
</tr>
<tr>
<td>Maximum External Call Control Diversion Hops to Pattern or DN</td>
<td>This parameter specifies the maximum number of times that the adjunct route server can issue the divert obligation for a call to a directory number, route pattern, translation pattern, or hunt pilot. The default is 12; the minimum is 1, and the maximum is 60.</td>
</tr>
<tr>
<td>External Call Control Routing Request Timer</td>
<td>This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager should wait for the call routing directive from the adjunct route server before allowing or blocking the call, as configured in the Call Treatment on Failures setting in the external call control profile. The default is 2000; the minimum value is 1000, and the maximum value is 5000.</td>
</tr>
<tr>
<td>External Call Control Fully Qualified Role And Resource</td>
<td>This parameter specifies the fully qualified role and the resource that Cisco Unified Communications Manager sends to the adjunct route server in the XACML call routing request. The value that you enter matches your configuration on the adjunct route server, and it ensures that the Cisco Unified Communications Manager query points to the correct routing rules on the adjunct route server. The default equals CISCO:UC:UCMPolicy:VoiceOrVideoCall, where CISCO:UC:UCMPolicy represents the role on the adjunct route server and VoiceOrVideoCall represents the resource on the adjunct route server. You can enter up to 100 characters, which include alphanumeric characters (A-Z,a-z,0-9) or colons (:). Colons are only allowed between alphanumeric characters.</td>
</tr>
</tbody>
</table>
Configuring External Call Control

External Call Control Feature Configuration Settings

Cisco Unified Communications Manager, Release 8.0(2) (or higher), supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied.

The external call control profile provides the URI(s) for the adjunct route server(s), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Call Control Initial Connection Count To PDP</td>
<td>This parameter specifies the initial number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests. Ensure that the value for this parameter is less than or equal to the External Call Control Maximum Connection Count To PDP value. If it is not less than or equal to the External Call Control Maximum Connection Count To PDP value, the External Call Control Maximum Connection Count To PDP value gets ignored. This setting applies to each URI that is configured in each external call control profile. The default is 2; the minimum value is 2, and the maximum value is 20.</td>
</tr>
<tr>
<td>External Call Control Maximum Connection Count To PDP</td>
<td>This parameter specifies the maximum number of connections that Cisco Unified Communications Manager establishes to a adjunct route server for handling call routing requests. Ensure that the value for this parameter is greater than or equal to the External Call Control Initial Connection Count To PDP value. If it is not greater than the External Call Control Initial Connection Count To PDP value, the value gets ignored. This setting applies to each URI that is configured in each external call control profile. The default is 4; the minimum value is 2, and the maximum value is 20.</td>
</tr>
</tbody>
</table>
Table 22-4 describes the settings that display in the External Call Control Profile window (Call Routing > External Call Control Profile).

**Before You Begin**

Before you configure the external call control profile, configure a calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager. (Call Routing > Class of Control > Calling Search Space)

Before you configure the external call control profile, review the “Configuration Checklist for External Call Control” section on page 22-2.

**Next Step**

After you configure the external call control profile, assign the profile to the translation pattern. (Call Routing > Translation Pattern)

**Table 22-4 External Call Control Profile Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the external call control profile. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank spaces. The name that you enter displays in the Find and List External Call Control Profile window and in the External Call Control Profile drop-down list box in the Translation Pattern Configuration window.</td>
</tr>
<tr>
<td>Primary Web Service</td>
<td>Enter the URI for the primary adjunct route server, which is the adjunct route server where Cisco Unified Communications Manager sends routing queries to determine how to handle the call. You can enter http or https in this field. If you enter https, you must import a self-signed certificate from the adjunct route server, and you must export a Cisco Unified Communications Manager self-signed certificate to the adjunct route server. Enter the URI by using the following formula: https://&lt;hostname or IPv4 address of primary route server&gt;:&lt;port that is configured on primary route server&gt;/path from route server configuration. For example, enter <a href="https://primaryrouteserver:8443/pdp/AuthenticationEndPoint">https://primaryrouteserver:8443/pdp/AuthenticationEndPoint</a> If you use https, make sure that you enter the hostname that exists in the certificate in this field. (for example, the CN or Common Name in the certificate)</td>
</tr>
</tbody>
</table>
### Configuring External Call Control

Secondary Web Service
Enter the URI for the redundant adjunct route server, which is the redundant adjunct route server where Cisco Unified Communications Manager sends routing queries to determine how to handle the call. The secondary web service is optional and gets used for load balancing between the primary and secondary route servers if you check the Enable Load Balancing check box. Configuring a secondary web service also ensures redundancy; that is, that an active/standby link is available.

You can enter http or https in this field. If you enter https, you must import a self-signed certificate from the adjunct route server, and you must export a Cisco Unified Communications Manager self-signed certificate to the adjunct route server. If you use https, make sure that you enter the hostname that exists in the certificate in this field.

Enter the URI by using the following formula:
https://<hostname or IPv4 address of secondary route server>:<port that is configured on secondary route server>/path from route server configuration

For example, enter https://secondaryroutesserver:8443/pdp/AuthenticationEndPoint

If you use https, make sure that you enter the hostname that exists in the certificate in this field (for example, the CN or Common Name in the certificate)

Enable Load Balancing
If you want load balancing to occur between the primary and redundant adjunct route server, check this check box. If checked, load balancing occurs in a round robin fashion.

---

### Table 22-4 External Call Control Profile Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Web Service</td>
<td>Enter the URI for the redundant adjunct route server, which is the redundant adjunct route server where Cisco Unified Communications Manager sends routing queries to determine how to handle the call. The secondary web service is optional and gets used for load balancing between the primary and secondary route servers if you check the Enable Load Balancing check box. Configuring a secondary web service also ensures redundancy; that is, that an active/standby link is available. You can enter http or https in this field. If you enter https, you must import a self-signed certificate from the adjunct route server, and you must export a Cisco Unified Communications Manager self-signed certificate to the adjunct route server. If you use https, make sure that you enter the hostname that exists in the certificate in this field (for example, the CN or Common Name in the certificate)</td>
</tr>
<tr>
<td>Enable Load Balancing</td>
<td>If you want load balancing to occur between the primary and redundant adjunct route server, check this check box. If checked, load balancing occurs in a round robin fashion.</td>
</tr>
</tbody>
</table>
### Configuring External Call Control

#### Routing Request Timer
This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager should wait for the call routing directive from the adjunct route server before allowing or blocking the call, as configured in the Call Treatment on Failures setting in the external call control profile.

The default is 2000; the minimum value is 1000, and the maximum value is 5000.

If this field is left blank, Cisco Unified Communications Manager uses the configuration for the External Call Control Routing Request Timer service parameter, which supports the Cisco CallManager service.

#### Diversion Rerouting Calling Search Space
From the drop-down list box, choose the calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager.

#### Call Treatment on Failure
From the drop-down list box, choose whether Cisco Unified Communications Manager allows or blocks calls under the following circumstances:

- When the adjunct route server does not send the call routing directive to Cisco Unified Communications Manager
- When Cisco Unified Communications Manager cannot contact the adjunct route server
- When Cisco Unified Communications Manager fails to parse the routing directive (or supplements of the routing directive)
- When Cisco Unified Communications Manager receives a 4xx or 5xx message from the adjunct route server

Choosing **Allow Calls** routes the call to the current destination, as if the adjunct route server issued a Permit decision with Continue obligation.

Choosing **Block Calls** causes Cisco Unified Communications Manager to clear the call, as if the adjunct route server issued a Deny decision with a Reject obligation.

When failure occurs, an alarm gets logged.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Request Timer</td>
<td>This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager should wait for the call routing directive from the adjunct route server before allowing or blocking the call, as configured in the Call Treatment on Failures setting in the external call control profile. The default is 2000; the minimum value is 1000, and the maximum value is 5000. If this field is left blank, Cisco Unified Communications Manager uses the configuration for the External Call Control Routing Request Timer service parameter, which supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Diversion Rerouting Calling Search Space</td>
<td>From the drop-down list box, choose the calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
| Call Treatment on Failure          | From the drop-down list box, choose whether Cisco Unified Communications Manager allows or blocks calls under the following circumstances:  

- When the adjunct route server does not send the call routing directive to Cisco Unified Communications Manager  
- When Cisco Unified Communications Manager cannot contact the adjunct route server  
- When Cisco Unified Communications Manager fails to parse the routing directive (or supplements of the routing directive)  
- When Cisco Unified Communications Manager receives a 4xx or 5xx message from the adjunct route server  

Choosing **Allow Calls** routes the call to the current destination, as if the adjunct route server issued a Permit decision with Continue obligation.  
Choosing **Block Calls** causes Cisco Unified Communications Manager to clear the call, as if the adjunct route server issued a Deny decision with a Reject obligation.  
When failure occurs, an alarm gets logged. |
Finding Configuration Records for External Call Control Profiles

Cisco Unified Communications Manager supports the external call control feature, which enables an adjunct route server to make call-routing decisions for Cisco Unified Communications Manager by using the 8.0(2) Cisco Unified Routing Rules Interface. When you configure external call control, Cisco Unified Communications Manager issues a route request that contains the calling party and called party information to the adjunct route server. The adjunct route server receives the request, applies appropriate business logic, and returns a route response that instructs Cisco Unified Communications Manager on how the call should get routed, along with any additional call treatment that should get applied.

The adjunct route server can instruct Cisco Unified Communications Manager to allow, divert, or deny the call, modify calling and called party information, play announcements to callers, reset call history so adjunct voicemail and IVR servers can properly interpret calling/called party information, and log reason codes that indicate why calls were diverted or denied.

Tip

Be aware that routing rules and business logic on the adjunct route server determine how the call is handled. If your configuration in Cisco Unified Communications Manager Administration conflicts with the routing rule, the routing rule gets used for the call.

To locate external call control profiles in Cisco Unified Communications Manager Administration, perform the following procedure:

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Call Routing > External Call Control Profile.

Step 2  The Find and List window displays. Records from an active (prior) query may also display in the window.

Step 3  To find all records in the database, ensure the dialog box is empty; go to Step 4.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4  Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configured records for this selection by clicking Select All and then clicking Delete Selected.
Step 5  From the list of records that display, click the link for the record that you want to view.

Note  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Related Topics” section on page 22-23.

Configuring an External Call Control Profile

External call control, which is a rules-based routing feature, requires that Cisco Unified Communications Manager send call-routing queries to an adjunct route server before routing the call. Routing rules that are set on the adjunct route server determine how the call gets handled. The adjunct route server uses the Cisco Unified Routing Rules XML interface to communicate with Cisco Unified Communications Manager. After the adjunct route server receives the query from Cisco Unified Communications Manager, the adjunct route server directs Cisco Unified Communications Manager on how to handle the call.

Tip  Be aware that routing rules and business logic on the adjunct route server determine how the call is handled. If your configuration in Cisco Unified Communications Manager Administration conflicts with the routing rule, the routing rule gets used for the call.

The external call control profile provides the URIs for the adjunct route server(s), a calling search space that is used for diverting calls, a timer that indicates how long Cisco Unified Communications Manager waits for a response from the adjunct route server, and so on.

Before You Begin
Before you configure the external call control profile, configure a calling search space that Cisco Unified Communications Manager uses when the adjunct route server sends a divert obligation to Cisco Unified Communications Manager.

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Call Routing > External Call Control Profile.

Step 2  From the Find and List window, perform one of the following tasks:

- To copy an existing record related to external call control profiles, locate the record as described in the “Finding Configuration Records for External Call Control Profiles” section on page 22-19, click the Copy button next to the record that you want to copy, and continue with Step 3.
- To add a new external call control profile, click the Add New button and continue with Step 3.
- To update an existing external call control profile, locate the appropriate record as described in the “Finding Configuration Records for External Call Control Profiles” section on page 22-19 and continue with Step 3.
**Step 3**
Configure the appropriate fields, as described in Table 22-4.

**Step 4**
To save the configuration information to the database, click **Save**.

---

**Next Step**
Assign the external call control profile to the translation pattern.

**Additional Information**
See the “Related Topics” section on page 22-23.

---

**Assigning the External Call Control Profile to the Translation Pattern**

To assign the external call control profile to the translation pattern in Cisco Unified Communications Manager Administration, choose **Call Routing > Translation Pattern**. In the Translation Pattern Configuration window, choose the external call control profile that you want to assign to the pattern from the External Call Control Profile drop-down list box.

---

**Deleting Configuration Records for External Call Control Profiles**

This section describes how to delete a configured external call control profile in Cisco Unified Communications Manager Administration.

---

**Note**
You can delete multiple records from the Find and List window by checking the check boxes next to the appropriate records and clicking **Delete Selected**. You can delete all records in the window by clicking **Select All** and then clicking **Delete Selected**.

---

**Before You Begin**
Before you can delete the external call control profile, you must unassign the profile from the translation pattern(s) that refer(s) to it. If you attempt to delete a profile that is assigned to a translation pattern, an error message displays in Cisco Unified Communications Manager Administration.

---

**Procedure**

**Step 1**
If you want to delete the record from the Find and List window, perform the following tasks:

1. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for External Call Control Profiles” section on page 22-19.
2. Click the record that you want to delete.
3. Click **Delete Selected**.
   - You receive a message that asks you to confirm the deletion.
4. Click **OK**.
   - The window refreshes, and the record gets deleted from the database.
If you want to delete the record from the configuration window, perform the following tasks:

a. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for External Call Control Profiles” section on page 22-19.

b. Access the configuration window; click Delete in the configuration window.
   You receive a message that asks you to confirm the deletion.

c. Click OK.
   The window refreshes, and the record gets deleted from the database.

Additional Information
See the “Related Topics” section on page 22-23.

Importing the Adjunct Route Server Certificate

If you specify https for the primary or secondary web service URIs in the external call control profile in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager uses certificates to mutually authenticate via a TLS connection to the adjunct route server(s).

To import the self-signed certificate for the adjunct route server into the Cisco Unified Communications Manager trusted store, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Operating System, choose Security > Certificate Management.

Step 2 In the Certificate List window, click Upload Certificate.

Step 3 When the Upload Certificate popup window displays, choose CallManager-trust from the Certificate Name drop-down list box, and browse to the certificate for the adjunct route server; after the certificate displays in the Upload File field, click the Upload File button.

Step 4 Perform this procedure again if Cisco Unified Communications Manager can contact a redundant adjunct route server.

Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export

To ensure that the primary and redundant route servers can authenticate with Cisco Unified Communications Manager through https, you must generate a self-signed certificate that you can import to each adjunct route server that sends directives to Cisco Unified Communications Manager.

You do not need to perform this procedure if the adjunct route server uses http, as indicated in the external call control profile in Cisco Unified Communications Manager Administration.

To generate a Cisco Unified Communications Manager self-signed certificate that you can export to adjunct route server, perform the following procedure:
Providing Information to End Users

Because limitations and restrictions exist for chaperones, notify users that you designated as chaperones.

Troubleshooting External Call Control

For information on troubleshooting external call control, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Related Topics

- Configuration Checklist for External Call Control, page 22-2
- Introducing External Call Control for Cisco Unified Communications Manager, page 22-5
- System Requirements for External Call Control, page 22-10
- Interactions and Restrictions, page 22-10
- Installing and Activating External Call Control, page 22-13
  - Configuring External Call Control, page 22-13
  - Service Parameters for External Call Control, page 22-13
  - External Call Control Profile Configuration Settings, page 22-15
  - Finding Configuration Records for External Call Control Profiles, page 22-19
  - Configuring an External Call Control Profile, page 22-20
  - Assigning the External Call Control Profile to the Translation Pattern, page 22-21
  - Deleting Configuration Records for External Call Control Profiles, page 22-21
  - Importing the Adjunct Route Server Certificate, page 22-22
  - Generating a Cisco Unified Communications Manager Self-Signed Certificate For Export, page 22-22
Related Topics

- Providing Information to End Users, page 22-23
- Troubleshooting External Call Control, page 22-23
- Announcement Configuration, *Cisco Unified Communications Manager Administration Guide*
External Call Transfer Restrictions

External Call Transfer Restrictions feature allows you to configure gateways, trunks, and route patterns as OnNet (internal) or OffNet (external) devices at the system level. By setting the devices as OffNet, you can restrict the transferring of an external call to an external device and thus help prevent toll fraud.

This chapter provides the following information about external call transfer restrictions:

- Configuration Checklist for External Call Transfer Restrictions, page 23-1
- Introducing External Call Transfer Restrictions, page 23-2
- System Requirements for External Call Transfer Restrictions, page 23-5
- Interactions and Restrictions, page 23-5
- Installing and Activating External Call Transfer Restrictions, page 23-6
- Configuring External Call Transfer Restrictions, page 23-6
- Related Topics, page 23-9

Configuration Checklist for External Call Transfer Restrictions

The External Call Transfer Restrictions feature allows you to configure gateways, trunks, and route patterns as OnNet (internal) or OffNet (external) devices at the system level. By setting the devices as OffNet, you can restrict the transferring of an external call to an external device and thus help prevent toll fraud.
Introducing External Call Transfer Restrictions

External call transfer restrictions block call transfer between external parties. Setting service parameters and configuring gateways, trunks, and route patterns as OffNet (external) devices provide external call transfer blocking. This feature provides an OnNet or OffNet alerting tone to the terminating end of the call (determined by the configuration of the device as either OnNet or OffNet, respectively). This chapter uses the following terms:

- **OnNet Device**—A device that is configured as OnNet and considered to be internal to the network.
- **OffNet Device**—A device that is configured as OffNet and, when routed, is considered to be external to the network.
- **Network Location**—The location of the device, which is considered as OnNet or OffNet, with respect to the network.

Table 23-1 provides a checklist to configure external call transfer restrictions. For more information on external call transfer restrictions, see the “Introducing External Call Transfer Restrictions” section on page 23-2 and the “Related Topics” section on page 23-9.

**Table 23-1  External Call Transfer Restrictions Configuration Checklist**

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>To block external calls from being transferred to external devices, perform the following steps:</td>
<td>Setting the Block OffNet to OffNet Transfer Service Parameter, page 23-7</td>
</tr>
<tr>
<td>1. Set the Block OffNet to OffNet Transfer clusterwide service parameter to True.</td>
<td>Configuring Transfer Capabilities by Using Gateway Configuration, page 23-8</td>
</tr>
<tr>
<td>2. For incoming calls, configure individual gateways or trunks as OffNet.</td>
<td>Configuring Transfer Capabilities by Using Trunk Configuration, page 23-8</td>
</tr>
<tr>
<td>3. For outgoing calls, configure route pattern Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements (for example, if the check box is checked, the setting on the associated gateway or trunk is considered; if it is unchecked, the call classification value of the route pattern classifies the call).</td>
<td>Route Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>To configure all gateways or trunks to be OffNet (external) or OnNet (internal), perform the following steps:</td>
<td>Configuring Transfer Capabilities by Using Call Classification Service Parameter, page 23-7</td>
</tr>
<tr>
<td>1. Set the Cisco Unified Communications Manager clusterwide service parameter Call Classification to OffNet (if all gateways and trunks are to be external) or OnNet (if all gateways and trunks are to be internal).</td>
<td>Configuring Transfer Capabilities by Using Gateway Configuration, page 23-8</td>
</tr>
<tr>
<td>2. Configure individual gateways or trunks to Use System Default in the Call Classification field.</td>
<td>Configuring Transfer Capabilities by Using Trunk Configuration, page 23-8</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>On the Route Pattern Configuration window, set the Call Classification field as OffNet. The Allow Device Override check box can be checked or unchecked, depending on the requirements and the configurations of the gateway or trunk.</td>
<td>Route Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
• Originating End—The device that gets transferred. The system considers this device as OnNet or OffNet.
• Terminating End—The device that receives the transferred call. The system considers this device as OnNet or OffNet.
• Incoming Call—A call for which only gateways and trunks call classification settings get used to classify it as OnNet or OffNet. Route Pattern call classification settings do not apply.
• Outgoing Call—A call for which the call classification setting of the trunk, gateway, and route pattern gets considered. The Allow Device Override setting on the route pattern determines whether the trunk or gateway call classification setting gets used instead of the route pattern call classification setting.

**Gateways and Trunks**
You can configure gateways and trunks as OnNet (internal) or OffNet (external) by using Gateway Configuration or Trunk Configuration or by setting a clusterwide service parameter. When the feature is used in conjunction with the clusterwide service parameter Block OffNet to OffNet Transfer, the configuration determines whether calls can transfer over a gateway or trunk.

You can configure the following devices as internal and external to Cisco Unified Communications Manager:
• H.323 gateway
• MGCP FXO trunk
• MGCP T1/E1 trunk
• Intercluster trunk
• SIP trunk

**Route Patterns**
To classify a call as OnNet or OffNet, administrators can set the Call Classification field to OnNet or OffNet, respectively, on the Route Pattern Configuration window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box on the Route Pattern Configuration window.

For more information, see the “Configuring External Call Transfer Restrictions” section on page 23-6.

**Example**
The following example illustrates how callers use transfer to avoid paying for long-distance calls. In Figure 23-1, Party A from ABC Company in New York calls Party B, a friend in New Zealand. After the call connects, Party A transfers the call to Party C, another friend who lives in England. When transfer completes, Party B and Party C are connected, and Party A gets disconnected. As a result, ABC Company gets billed for the call between New Zealand and England.
Introducing External Call Transfer Restrictions

In Figure 23-1, the system prevents transferring an external call to an external party because, regardless of how the gateway or trunk is configured, the route pattern was configured as OffNet, and the service parameter Block OffNet to OffNet Transfer is set to True.

In Figure 23-2, the system prevents transferring an external call to an external party because, regardless of how the gateway or trunk is configured, the route pattern was configured as OffNet, and the service parameter Block OffNet to OffNet Transfer is set to True.
System Requirements for External Call Transfer Restrictions

The external call transfer restriction requires the following software component to operate:

- Cisco Unified Communications Manager 5.0 or later

Interactions and Restrictions

The following sections describe the interactions and restrictions for external call transfer restrictions:

- Interactions, page 23-5
- Restrictions, page 23-6

Interactions

The following sections describe how external call transfer restrictions feature interacts with Cisco Unified Communications Manager applications and call processing.
Drop Conference
The Drop Conference feature determines whether an existing ad hoc conference should be dropped by checking whether the conference parties are configured as OffNet or OnNet. You use the service parameter Drop Ad Hoc Conference and choose the option When No OnNet Parties Remain in the Conference to configure the feature. You determine OnNet status for each party by checking the device or route pattern that the party is using. For more information, see “Ad Hoc Conference Linking” in the Cisco Unified Communications Manager System Guide.

Bulk Administration
Bulk Administration inserts gateway configuration (OffNet or OnNet) on the Gateway Template. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

Dialed Number Analyzer (DNA)
When used to perform digit analysis on a gateway, DNA displays the Call Classification that is configured for the gateway and the route pattern. See the Cisco Unified Communications Manager Dialed Number Analyzer Guide for more information.

Restrictions
The following restrictions apply to external call transfer restrictions:

- FXS gateways such as Cisco Catalyst 6000 24 Port do not have a Call Classification field on the Gateway Configuration window; therefore, the system always considers them as OnNet.
- The system does not support the Cisco VG-248 Gateway which does not have a Call Classification field.
- Cisco Unified Communications Manager considers all Cisco Unified IP Phones and FXS ports as OnNet (internal) that cannot be configured as OffNet (external).

Installing and Activating External Call Transfer Restrictions
To activate external call transfer restrictions, perform the following steps:

1. Set the Block OffNet to OffNet Transfer service parameter to True.
2. In Route Pattern Configuration window, set the Call Classification field to OffNet. Leave the Allow Device Override check box unchecked, so the device uses the Call Classification setting of the route pattern.
3. Configure the trunks and gateways that you want to be identified as OffNet.

See the “Configuring External Call Transfer Restrictions Service Parameters” section on page 23-7 for details.

Configuring External Call Transfer Restrictions
This section contains the following information:

- Configuring External Call Transfer Restrictions Service Parameters, page 23-7
- Configuring Transfer Capabilities by Using Gateway Configuration, page 23-8
Configuring External Call Transfer Restrictions Service Parameters

You can set two service parameters for the external call transfer restrictions feature: Call Classification and Block OffNet to OffNet Transfer. The following sections provide configuration information:

- Configuring Transfer Capabilities by Using Call Classification Service Parameter, page 23-7
- Setting the Block OffNet to OffNet Transfer Service Parameter, page 23-7

Configuring Transfer Capabilities by Using Call Classification Service Parameter

To configure all gateways or trunks in the Cisco Unified Communications Manager cluster to be OffNet (external) or OnNet (internal), perform the following two steps:

1. Using the Cisco Unified Communications Manager clusterwide service parameter Call Classification, choose either OffNet or OnNet (the default specifies OffNet).
2. In the Call Classification field on the Gateway Configuration and Trunk Configuration windows, configure each gateway and trunk to Use System Default (this reads the setting in the Call Classification service parameter and uses that setting for the gateway and trunk).

Additional Information
See the “Related Topics” section on page 23-9.

Setting the Block OffNet to OffNet Transfer Service Parameter

The Cisco Unified Communications Manager clusterwide service parameter Block OffNet to OffNet Transfer allows administrators to prevent users from transferring external calls to another external number. This parameter specifies values as True or False. Setting the parameter to True blocks external calls from being transferred to another external device. The default value specifies False. You modify the Block OffNet to OffNet Transfer service parameter by using the Service Parameter Configuration window.

When a user tries to transfer a call on an OffNet gateway or trunk when the service parameter Block OffNet to OffNet Transfer is set to True, a message displays on the user phone to indicate that the call cannot be transferred.

Additional Information
See the “Related Topics” section on page 23-9.
Configuring Transfer Capabilities by Using Gateway Configuration

To configure the gateway as OffNet, OnNet, or Use System Default, perform the following procedure. The system considers calls that come to the network through that gateway as OffNet or OnNet, respectively.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified Communications Manager Administration, choose <strong>Device &gt; Gateway</strong>. The Find and List Gateways window displays.</td>
</tr>
<tr>
<td>Step 2</td>
<td>To list the configured gateways, click <strong>Find</strong>. The gateways that are configured in Cisco Unified Communications Manager display.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the gateway that you want to configure as OffNet or OnNet.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Call Classification field, choose the setting. See Table 23-2 for a description of these settings.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**Table 23-2** Call Classification Configuration Settings

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OffNet</td>
<td>This setting identifies the gateway as an external gateway. When a call comes in from a gateway that is configured as OffNet, the system sends the outside ring to the destination device.</td>
</tr>
</tbody>
</table>
Configuring Transfer Capabilities by Using Route Pattern Configuration

The Route Pattern Configuration window provides the following fields:

- **Call Classification**—Use this drop-down list box to classify the call that uses this route Pattern as OffNet or OnNet.
- **Provide Outside Dial Tone**—If Call Classification is set to OffNet, this check box gets checked.
- **Allow Device Override**—When this check box is checked, the system uses the Call Classification setting of the trunk or gateway that is associated with the route pattern instead of the Call Classification setting on the Route Pattern Configuration window.

**Additional Information**

See the “Related Topics” section on page 23-9.

**Table 23-2  Call Classification Configuration Settings (continued)**

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnNet</td>
<td>This setting identifies the gateway as an internal gateway. When a call comes in from a gateway that is configured as OnNet, the system sends inside ring to the destination device.</td>
</tr>
<tr>
<td>Use System Default</td>
<td>This setting uses the Cisco Unified Communications Manager clusterwide service parameter Call Classification.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuration Checklist for External Call Transfer Restrictions, page 23-1
- Introducing External Call Transfer Restrictions, page 23-2
- System Requirements for External Call Transfer Restrictions, page 23-5
- Interactions and Restrictions, page 23-5
- Installing and Activating External Call Transfer Restrictions, page 23-6
- Configuring External Call Transfer Restrictions, page 23-6
- Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Trunk Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Conference Bridges, Cisco Unified Communications Manager System Guide

**Additional Cisco Documentation**

- Cisco Unified Communications Manager Dialed Number Analyzer Guide
- Cisco Unified Communications Manager Bulk Administration Guide
Geolocations and Location Conveyance

This chapter discusses the following concepts:
- Geolocations
- Geolocation filters
- Location conveyance

Do not confuse locations with geolocations. Locations, which you configure by using the System > Location menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the System > Geolocation Configuration menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

This chapter contains information on the following topics:
- Configuration Checklist for Geolocations, page 24-1
- Configuration Checklist for Geolocation Filters, page 24-3
- Configuration Checklist for Location Conveyance, page 24-4
- Introducing Geolocations, page 24-5
- Geolocation Interactions, page 24-9
- Geolocation Configuration, page 24-10
- Introducing Geolocation Filters, page 24-16
- Geolocation Filter Configuration, page 24-17
- Introducing Location Conveyance, page 24-21
- Location Conveyance Configuration, page 24-25
- Related Topics, page 24-25

Configuration Checklist for Geolocations

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.

Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.
Chapter 24  Geolocations and Location Conveyance

The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC.

In Cisco Unified Communications Manager Administration, geolocations get configured manually.

Tip

Do not confuse locations with geolocations. Locations, which you configure by using the **System > Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System > Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Table 24-1 provides a checklist for configuring geolocations. For more information on geolocations, see the “Introducing Geolocations” section on page 24-5 and the “Related Topics” section on page 24-25.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Define a set of geolocations on a new Geolocation Configuration window.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.</td>
</tr>
</tbody>
</table>

Geolocation Configuration, page 24-10

Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide

Gateway Configuration Settings, Cisco Unified Communications Manager Administration Guide

Displaying the MAC Address of a Phone, Cisco Unified Communications Manager Administration Guide

Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide
Table 24-1Geolocation Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.</td>
</tr>
<tr>
<td></td>
<td>Geolocation Configuration, page 24-10</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>For devices that do not participate in features that require geolocations, define the geolocation as Unspecified or leave undefined.</td>
</tr>
<tr>
<td>Note</td>
<td>You can define this lack of association at the individual-device level, the device-pool level, or the enterprise-parameter level.</td>
</tr>
<tr>
<td></td>
<td>Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Gateway Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Displaying the MAC Address of a Phone, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>

Additional Information
See the “Related Topics” section on page 24-25.

### Configuration Checklist for Geolocation Filters

Cisco Unified Communications Manager administrators define a geolocation filter for every device that participates in a feature that uses geolocation filters. Geolocation filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

Use the **System > Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.
Table 24-2 provides a checklist for configuring geolocation filters. For more information on geolocation filters, see the “Introducing Geolocation Filters” section on page 24-16 and the “Related Topics” section on page 24-25.

Table 24-2  
Geolocation Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Define a set of filter rules in a new Geolocation Filter Configuration window.</td>
<td>Geolocation Filter Configuration, page 24-17</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.</td>
<td>Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide&lt;br&gt;Gateway Configuration Settings, Cisco Unified Communications Manager Administration Guide&lt;br&gt;Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;For the logical partitioning feature, assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.</td>
<td>Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide&lt;br&gt;Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
</tbody>
</table>

Additional Information
See the “Related Topics” section on page 24-25.

Configuration Checklist for Location Conveyance

Location conveyance involves configuration to make the following behavior possible:

- Communicate geolocation information across clusters
- Allow communication of geolocation information from one cluster to another, at call establishment as well as midcall joins and redirects.

Note
 Enterprise parameters and logical partitioning configuration do not control location conveyance. If a device that communicates through a trunk associates with geolocation information, check the Send Geolocation Information check box when you configure the trunk (either SIP or ICT) to convey the geolocation information across clusters.

For the logical partitioning feature in the current release, the Cisco Unified Communications Manager does not send the configured geolocation information to line devices (phones that are running SIP or SCCP).
Introducing Geolocations

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.

Table 24-3 provides a checklist for configuring location conveyance in a multicloud logical partitioning environment.

### Table 24-3 Location Conveyance Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Geolocation Configuration, page 24-10</strong></td>
</tr>
<tr>
<td>Define a set of geolocations in a new Geolocation Configuration window.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Device Pool Configuration Settings,Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>Assign geolocations to device pools, devices, SIP trunks, intercluster trunks, gateways, or MGCP ports for the devices that need to participate in location conveyance.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Geolocation Configuration, page 24-10</strong></td>
</tr>
<tr>
<td>Assign geolocations to a default geolocation that the Default Geolocation enterprise parameter specifies. This assignment allows you to specify a default geolocation for a cluster. For devices for which no associated geolocation exists at the device or device-pool level, the value that is specified by the Default Geolocation enterprise parameter applies.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide</strong></td>
</tr>
<tr>
<td>If geolocation information about devices needs to be communicated across clusters, ensure that location conveyance is configured. To do so, check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk for the devices that need to pass geolocation information across clusters as follows:</td>
<td></td>
</tr>
<tr>
<td>• Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster.</td>
<td></td>
</tr>
<tr>
<td>• Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Information**

See the “Related Topics” section on page 24-25.
Introducing Geolocations

Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.

The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC.

In Cisco Unified Communications Manager Administration, geolocations get configured manually.

Tip

Do not confuse locations with geolocations. Locations, which you configure by using the System > Location menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the System > Geolocation Configuration menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Overview of Geolocations

Configuration of geolocations entails provisioning the following elements:

- Configure geolocation identifiers
  - You can define sets of geolocations (civic addresses).
  - You can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
  - You can define geolocation filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.

Additional Information

See the “Related Topics” section on page 24-25.

Geolocation Characteristics

Cisco Unified Communications Manager administrators must define the following item:

- A geolocation for every device that participates in any feature that requires geolocations. The Request for Comments (RFC) 4119 standard provides the basis for geolocations. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC. Geolocations get configured manually.

Cisco Unified Communications Manager administrators then assign geolocations to devices.

The following entities in a Cisco Unified Communications Manager cluster can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports
Introducing Geolocations

Note

Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

You do not need to associate media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, with geolocations.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The intercluster trunk (ICT) or SIP trunk device layer that receives this information uses the information for location conveyance.
4. No communication of geolocation from Cisco Unified Communications Manager to a phone takes place.

Source of Geolocation Information

The following logic determines the geolocation value:

1. Read the value for geolocation from the device window. If it is not configured on device page, for phone device in roaming, read the device pool (DP) from the roaming configuration. For phone device that is not in roaming, read the DP from the device configuration.
2. For trunk, ICT, or MGCP port device, read the DP from the device configuration.
3. From the selected DP, read the value of geolocation from DP configuration window.
4. If DP is not configured with a value for Geolocation, use blank value.
5. If available geolocation value is blank, call processing uses the configured value that the Default Geolocation enterprise parameter specifies.

The standard record for a geolocation specifies Unspecified. Use this value when no geolocation needs to associate with a device. In such scenarios, any features that are based on geolocations do not execute.

Also, devices for which no geolocation gets specified do not participate in geolocation information conveyance across clusters for intercluster calls.

Be aware that the Default Geolocation enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Additional Information

See the “Related Topics” section on page 24-25.
Introducing Geolocations

Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, you do not know the actual connected device until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- When a device answers, the actual geolocation information for the device becomes available and gets communicated to call control and to any features that are involved.

Geolocation Examples

Table 24-4 specifies examples of geolocations.

Table 24-4 Geolocation Examples

<table>
<thead>
<tr>
<th>Geolocation Name</th>
<th>Geolocation Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN-KA-BLR-BLD1</td>
<td>(country=IN, A1=KA, A3=Bangalore, A4= A4, A5=12, A6=Langford Road, PRD=12, LOC=BLD1, NAM=unified comm, PC=560001)</td>
</tr>
<tr>
<td>IN-KA-BLR-BLD2</td>
<td>(country=IN, A1=KA, A3=Bangalore, A4= A4, A6=Outer Ring Road, LOC=BLD2, NAM=unified comm, PC=560002)</td>
</tr>
<tr>
<td>IN-MH-MUM-BLD1</td>
<td>(country=IN, A1=MH, A3=Mumbai, A4= A4, LOC=blld1, NAM=unified comm, PC=220001)</td>
</tr>
<tr>
<td>IN-KA-BLR-ICTtoSJ</td>
<td>(country=IN, A1=KA, A3=Bangalore, NAM=ICTToSJ)</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 24-25.

Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

See the following sections for detailed descriptions of geolocations and geolocation filters:

- “Introducing Geolocations” section on page 24-5
- “Introducing Geolocation Filters” section on page 24-16

Geolocation filters allow selection of specific fields from the 17 geolocation fields. Use the System > Geolocation Filter menu option in Cisco Unified Communications Manager Administration to configure geolocation filters manually. Specific Cisco Unified Communications Manager features associate the geolocation filters by using drop-down list boxes in the configuration windows of the devices that get configured for a particular feature.
The Cisco Unified Communications Manager device type of a device specifies one of the following values:

- **Border**—Use this value to specify accessing PSTN trunks, intercluster trunks (ICTs), gateways, and MGCP ports.
- **Interior**—Use this value for VoIP phones or internal endpoints.

See Table 32-2 in the “Logical Partitioning” chapter for a detailed listing of the Cisco Unified Communications Manager devices that associate with the Border and Interior device types.

The following object specifies an example geolocation identifier:

```
{ geolocPkid=9dc76052-3a37-78c2-639a-1c02e8f5d3a2,
  filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal=, devType=8}
```

where:

- The `geolocVal` field gets used in cases where the Cisco Unified Communications Manager database does not reference the geolocation record but data for a geolocation comes from another source (for example, location conveyance PIDF-LO XML from a remote cluster).

  In such cases, Cisco Unified Communications Manager constructs the name value pair for the geolocation fields.

  **Example:** “country=US:A1=Texas:A3=Richardson:LOC=Building 6” where the value gets communicated through the `geolocVal` field.

**Note** In such a case, the `geolocPkid` is kept null and call control or features access the `geolocVal` field from a geolocation identifier.

The following string specifies the logical representation of a geolocation identifier:

```
```

**Note** This geolocation identifier gets constructed from the member fields of a geolocation identifier.

### Geolocation Interactions

The following interaction applies to geolocations:

- **Location conveyance**

See the “Introducing Location Conveyance” section on page 24-21 for a detailed discussion of location conveyance.

**Additional Information**

See the “Related Topics” section on page 24-25.
Geolocation Configuration

Tip
Before you configure geolocations, review the “Configuration Checklist for Geolocations” section on page 24-1 and the “Configuration Checklist for Geolocation Filters” section on page 24-3.

Use the System > Geolocation Configuration menu option in Cisco Unified Communications Manager Administration to configure geolocations.

Tip
Do not confuse locations with geolocations. Locations, which you configure by using the System > Location menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the System > Geolocation Configuration menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

To configure geolocations, see the following sections:
- Finding a Geolocation, page 24-10
- Configuring a Geolocation, page 24-11
- Deleting a Geolocation, page 24-12
- Geolocation Configuration Settings, page 24-12

Additional Information
See the “Related Topics” section on page 24-25.

Finding a Geolocation

Because you might have multiple geolocations in your network, Cisco Unified Communications Manager lets you search for geolocations on the basis of specified criteria. Follow these steps to search for a specific geolocations in the Cisco Unified Communications Manager database.

Note
During your work in a browser session, Cisco Unified Communications Manager Administration retains your geolocation search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your geolocation search preferences until you modify your search or close the browser.

Procedure

Step 1
Choose System > Geolocation Configuration.
The Find and List Geolocations window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
• From the second drop-down list box, choose a search pattern.
• Specify the appropriate search text, if applicable.

Note: To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.
All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note: You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

Note: To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Related Topics” section on page 24-25.

Configuring a Geolocation

Perform the following procedure to add or update a geolocation.

Procedure

Step 1  Choose System > Geolocation Configuration.
The Find and List Geolocations window displays.

Step 2  Perform one of the following tasks:
• To add a new geolocation, click Add New.
The Geolocation Configuration window displays.
• To update a geolocation, locate a specific geolocation as described in the “Finding a Geolocation” section on page 24-10.

Step 3  Enter the appropriate settings as described in Table 24-5.
Step 4 Click Save.
If you added a geolocation, the list box at the bottom of the window now includes the new geolocation.

Additional Information
See the “Related Topics” section on page 24-25.

Deleting a Geolocation

Perform the following procedure to delete an existing geolocation.

Procedure

Step 1 Choose System > Geolocation Configuration.
The Find and List Geolocations window displays.

Step 2 To locate a specific geolocation, enter search criteria and click Find.
A list of geolocations that match the search criteria displays.

Step 3 Perform one of the following actions:
• Check the check boxes next to the geolocations that you want to delete and click Delete Selected.
• Delete all geolocations in the window by clicking Select All and then clicking Delete Selected.
• From the list, choose the name of the geolocation that you want to delete and click Delete.
A confirmation dialog displays.

Step 4 Click OK.
The specified geolocation gets deleted.

Additional Information
See the “Related Topics” section on page 24-25.

Geolocation Configuration Settings

Geographical location information, or geolocation, describes a physical position in the world that may correspond to the past, present, or future location of a person, event, or device.
Cisco Unified Communications Manager Administration allows you to specify a geolocation for every device.
In Cisco Unified Communications Manager Administration, geolocations get configured manually.
Do not confuse locations with geolocations. Locations, which you configure by using the **System > Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System > Geolocation Configuration** menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

Table 24-5 describes the configuration settings that are used for configuring geolocations.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation Configuration Name</td>
<td>Enter a unique name for this geolocation. The name can contain up to 50 ASCII characters. You can use all characters except quotes (&quot;), close angle bracket (&gt;), open angle bracket (&lt;), backslash (%), and percent sign (%).</td>
</tr>
<tr>
<td>Geolocation Configuration Description</td>
<td>Enter a description for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Geolocation Configuration Country</td>
<td>Enter the two-letter country abbreviation for the country where this geolocation is located. Use the ISO 3166 code. The country must comprise two ASCII characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Geolocation Configuration State, Region, or Province (A1)</td>
<td>Enter a national subdivision for this geolocation, such as a state, region, province, or prefecture. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Geolocation Configuration County or Parish (A2)</td>
<td>Enter a county, parish, gun (JP), or district (IN) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
</tbody>
</table>

**Examples:**
- US for United States, IN for India
- Texas, Karnataka, Maharashtra
- Tarrant, Harris, Plaquemines
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>City or Township (A3)</td>
<td>Enter a city, township, or shi (JP) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> Bangladesh, New Delhi, Mumbai, Dallas, Tokyo, Sydney</td>
</tr>
<tr>
<td>Borough or City District (A4)</td>
<td>Enter a city division, borough, city district, ward, or chou (JP) for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> Manhattan, Brooklyn, Westminster, Hollywood</td>
</tr>
<tr>
<td>Neighborhood (A5)</td>
<td>Enter a neighborhood or block for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> Midtown, Soho, Southbank</td>
</tr>
<tr>
<td>Street (A6)</td>
<td>Enter a street for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> Main, Commerce, Champs-Elysees, Broadway</td>
</tr>
<tr>
<td>Leading Street Direction, such as N or W (PRD)</td>
<td>Enter a leading street direction for this geolocation. This field can contain up to 10 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> N, S, E, W (as in 43 N Wabash Avenue)</td>
</tr>
<tr>
<td>Trailing Street Suffix, such as SW (POD)</td>
<td>Enter a trailing street suffix for this geolocation. This field can contain up to 10 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> SW, NE, NW, SE (as in 245 E 45th St NW)</td>
</tr>
</tbody>
</table>
### Table 24-5  Geolocation Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Suffix, such as Avenue, Platz (STS)</td>
<td>Enter an address suffix for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Numeric house number (HNO)</td>
<td>Enter a numeric house number for this geolocation. This field can contain up to 10 numeric characters. Default value specifies blank.</td>
</tr>
<tr>
<td>House Number Suffix, such as A, 1/2 (HNS)</td>
<td>Enter a house number suffix for this geolocation. This field can contain up to 20 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Landmark (LMK)</td>
<td>Enter a landmark or vanity address for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Additional Location Information, such as Room Number (LOC)</td>
<td>Enter additional location information, such as a room number, for this geolocation. This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Floor (FLR)</td>
<td>Enter a floor for this geolocation. This field can contain up to 10 ASCII characters. Default value specifies blank.</td>
</tr>
</tbody>
</table>
## Introducing Geolocation Filters

Cisco Unified Communications Manager administrators define the following item:

- A geolocation filter for every device that participates in a feature that uses geolocation filters. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices.

The following logic determines the geolocation filter value:

1. For phone device that is in roaming, read the geolocation filter value from DP in roaming configuration. For phone device that is not in roaming, read the geolocation filter value from DP in device configuration.

2. For trunk, intercluster trunk, or MGCP port device, read geolocation filter value from device window. If no value is configured, read from DP.

3. If DP is not configured with a geolocation filter value, use blank value.

4. If available filter is blank, call processing uses the value that the Default Geolocation Filter enterprise parameter specifies.

### Additional Information

See the “Related Topics” section on page 24-25.

---

### Table 24-5 Geolocation Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Business or Resident (NAM)</td>
<td>Enter a business name or resident name or office occupant for this geolocation.</td>
</tr>
<tr>
<td></td>
<td>This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> Cisco Systems, Joe’s Barbershop</td>
</tr>
<tr>
<td>Zip or Postal Code (PC)</td>
<td>Enter a zip code or postal code for this geolocation.</td>
</tr>
<tr>
<td></td>
<td>This field can contain up to 20 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> 75042-0401, SW1V 1RP</td>
</tr>
</tbody>
</table>
Geolocation Filter Examples

Table 24-6 specifies examples of geolocation filters.

<table>
<thead>
<tr>
<th>Geolocation Name</th>
<th>Geolocation Filter Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>India-Filter1</td>
<td>(UseCountry, UseA1, UseA3, UseLOC)</td>
</tr>
<tr>
<td>India-GW-Filter2</td>
<td>(UseCountry, UseA1, UseA3, UseLOC, UseNAM)</td>
</tr>
<tr>
<td>India-ICT-Trunk-Filter3</td>
<td>(UseCountry, UseA1, UseA3, UseNAM)</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 24-25.

Geolocation Filter Configuration

Tip

Before you configure geolocations filters, review the “Configuration Checklist for Geolocation Filters” section on page 24-3.

Use the System > Geolocation Filter menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

To configure geolocation filters, see the following sections:

- Finding a Geolocation Filter, page 24-17
- Configuring a Geolocation Filter, page 24-18
- Deleting a Geolocation Filter, page 24-19
- Geolocation Filter Configuration Settings, page 24-20

Additional Information

See the “Related Topics” section on page 24-25.

Finding a Geolocation Filter

Because you might have multiple geolocation filters in your network, Cisco Unified Communications Manager lets you search for geolocation filters on the basis of specified criteria. Follow these steps to search for a specific geolocation filters in the Cisco Unified Communications Manager database.

Note

During your work in a browser session, Cisco Unified Communications Manager Administration retains your geolocation filter search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your geolocation filter search preferences until you modify your search or close the browser.
Geolocation Filter Configuration

Procedure

Step 1  Choose System > Geolocation Filter.

The Find and List Geolocation Filters window displays. Records from an active (prior) query may also display in the window.

Step 2  To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

Note  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information

See the “Related Topics” section on page 24-25.

Configuring a Geolocation Filter

Perform the following procedure to add or update a geolocation filter.

Procedure

Step 1  Choose System > Geolocation Filter.

The Find and List Geolocation Filters window displays.
Step 2 Perform one of the following tasks:
- To add a new geolocation filter, click **Add New**.
  The Geolocation Filter Configuration window displays.
- To update a geolocation filter, locate a specific geolocation filter as described in the “Finding a Geolocation Filter” section on page 24-17.

Step 3 Enter the appropriate settings as described in Table 24-7.

Step 4 Click **Save**.
If you added a geolocation filter, the list box at the bottom of the window now includes the new geolocation filter.

Additional Information
See the “Related Topics” section on page 24-25.

Deleting a Geolocation Filter

Perform the following procedure to delete an existing geolocation filter.

Procedure

Step 1 Choose **System > Geolocation Filter**.
The Find and List Geolocation Filters window displays.

Step 2 To locate a specific geolocation filter, enter search criteria and click **Find**.
A list of geolocation filters that match the search criteria displays.

Step 3 perform one of the following actions:
- Check the check boxes next to the geolocation filters that you want to delete and click **Delete Selected**.
- Delete all geolocation filters in the window by clicking **Select All** and then clicking **Delete Selected**.
- From the list, choose the name of the geolocation filter that you want to delete and click **Delete**.
A confirmation dialog displays.

Step 4 Click **OK**.
The specified geolocation filter gets deleted.

Additional Information
See the “Related Topics” section on page 24-25.
Geolocation Filter Configuration Settings

Cisco Unified Communications Manager administrators define the following item:

- A geolocation filter for every device that participates in a feature that uses geolocation filters. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation filters to devices. Table 24-7 describes the configuration settings that are used for configuring geolocation filters.

### Table 24-7  Geolocation Filter Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation Filter Configuration</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for this geolocation filter. Default name cannot be blank.</td>
</tr>
<tr>
<td></td>
<td>This field can contain up to 50 ASCII characters. You can use all characters except quotes (&quot;), close angle bracket (), open angle bracket (&lt;), backslash (), ampersand (&amp;), and percent sign (%).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this geolocation filter.</td>
</tr>
<tr>
<td></td>
<td>This field can contain up to 50 ASCII or unicode characters. Default value specifies blank.</td>
</tr>
<tr>
<td>Country using the two-letter abbreviation</td>
<td>Check this box to use the Country field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>State, Region, or Province (A1)</td>
<td>Check this box to use the State, Region, or Province (A1) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>County or Parish (A2)</td>
<td>Check this box to use the County or Parish (A2) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>City or Township (A3)</td>
<td>Check this box to use the City or Township (A3) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Borough or City District (A4)</td>
<td>Check this box to use the Borough or City District (A4) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Neighborhood (A5)</td>
<td>Check this box to use the Neighborhood (A5) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Street (A6)</td>
<td>Check this box to use the Street (A6) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Leading Street Direction, such as N or W (PRD)</td>
<td>Check this box to use the Leading Street Direction, such as N or W (PRD) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Trailing Street Suffix, such as SW (POD)</td>
<td>Check this box to use the Trailing Street Suffix, such as SW (POD) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Address Suffix, such as Avenue, Platz (STS)</td>
<td>Check this box to use the Address Suffix, such as Avenue, Platz (STS) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Numeric house number (HNO)</td>
<td>Check this box to use the Numeric house number (HNO) field of a specified geolocation to create this geolocation filter.</td>
</tr>
</tbody>
</table>
Introducing Location Conveyance

Location conveyance involves configuration to make the following behavior possible:

- Communicate geolocation information across clusters
  - Allow communication of geolocation information from one cluster to another, at call establishment as well as midcall joins and redirects.

Note

Enterprise parameters and logical partitioning configuration do not control location conveyance. If a device that communicates through a trunk associates with geolocation information, check the Send Geolocation Information check box when you configure the trunk (either SIP or ICT) to convey the geolocation information across clusters.

For the logical partitioning feature in the current release, the Cisco Unified Communications Manager does not send the configured geolocation information to line devices (phones that are running SIP or SCCP).

This section covers the following topics:

- Geolocation Conveyance Across SIP Trunks and Intercluster Trunks, page 24-22
- SIP Trunk Error Handling for Geolocation Information, page 24-22
- Intercluster Trunk Error Handling for Geolocation Information, page 24-23
- Handling a Received Geolocation, page 24-23
- Feature Interactions with Midcall Geolocation Change, page 24-23

Table 24-7 Geolocation Filter Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>House Number Suffix, such as A, 1/2 (HNS)</td>
<td>Check this box to use the House Number Suffix, such as A, 1/2 (HNS) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Landmark (LMK)</td>
<td>Check this box to use the Landmark (LMK) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Additional Location Information, such as Room Number (LOC)</td>
<td>Check this box to use the Additional Location Information, such as Room Number (LOC) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Floor (FLR)</td>
<td>Check this box to use the Floor (FLR) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Name of Business or Resident (NAM)</td>
<td>Check this box to use the Name of Business or Resident (NAM) field of a specified geolocation to create this geolocation filter.</td>
</tr>
<tr>
<td>Zip or Postal Code (PC)</td>
<td>Check this box to use the Zip or Postal Code (PC) field of a specified geolocation to create this geolocation filter.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 24-25.
Introducing Location Conveyance

Additional Information
See the “Related Topics” section on page 24-25.

Geolocation Conveyance Across SIP Trunks and Intercluster Trunks

Geolocation conveyance entails the following characteristics:

- Geolocation gets sent from one cluster to another.
- Geolocation information gets sent both at call establishment and at midcall joins and redirects.

The SIP trunk supports the location conveyance of Presence Information Data Format Location Object (PIDF-LO) as RFC 4119 describes, which specifies an encapsulation of location information within a presence document:

- Location conveyance supports the subset of SIP extension as specified in Location Conveyance draft-ietf-sip-location-conveyance-10.
- For communicating indication of device type, use User Agent Capability Presence Status, as specified in SIP extension draft-ietf-simple-prescaps-ext-08.
- Location conveyance supports the PIDF-LO in the <device> element as specified in SIP extension draft-ietf-geopriv-pdif-lo-profile-11.
- INVITE and UPDATE requests carry the PIDF-LO XML.
- Geolocation fields support ASCII and unicode characters.

Intercluster trunk also supports location conveyance that is using PIDF-LO XML with reduction in some of the XML elements:

- Elements include Setup, Alert, Progress, Connect, and Notify requests.
- Geolocation fields support ASCII characters.

The SIP trunk or intercluster trunk uses the geolocation information and device type that the call control messages send to construct the PIDF-LO XML.

SIP Trunk Error Handling for Geolocation Information

Incoming requests that carry geolocation information for location conveyance get checked for compliance as follows:

1. Geolocation headers indicate inclusion of PIDF-LO, but message body does not carry PIDF-LO.
2. Geolocation header has a CID header that refers to a URI for which no corresponding Content-ID header with the same URI exists.
3. Geolocation header has a URI other than CID header (for example, SIP or SIPS URI for LbyR).

The SIP trunk that receives a noncompliant SIP request responds with a “424 Bad Location Information” response.

The following cases result in ignoring the processing of geolocation info. For information purposes, the SIP trunk sends a Geolocation-Error header in the next outgoing SIP response (for example, 180 or 200):

- PIDF-LO lacks mandatory elements, such as “geopriv,” “location-info,” “civicAddress,” or “usage-rules.”
• If usage-rules show a retention-expiry time that already elapsed when it is compared to the current time in GMT, processing gets ignored.

Because the received geolocation information gets ignored, the SIP trunk continues to use the locally configured geolocation information on the SIP trunk.

Additional Information
See the “Related Topics” section on page 24-25.

Intercluster Trunk Error Handling for Geolocation Information

If an error occurs while the received geolocation information on an intercluster trunk is being processed, locally configured geolocation information for the trunk gets used.

Additional Information
See the “Related Topics” section on page 24-25.

Handling a Received Geolocation

The cluster that receives the PIDF-LO XML parses the received geolocation information and passes the information as colon-separated name value pairs in the GeolocationInfo data structure of the CeNotifyInd signal.


The content of the received geolocation information of the PIDF-LO overrides any locally configured geolocation information on a trunk, which gets used for the device across the trunk.

Example: {geolocPkid=, filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal="Country=US:A1=NC:A3=RTP:LOC=BLD9", devType=4}

Additional Information
See the “Related Topics” section on page 24-25.

Feature Interactions with Midcall Geolocation Change

Outgoing Geolocation Change
The supplementary service (SS) feature interactions, such as Transfer, Conference, Park retrieval, and others, result in connected party change.

For such scenarios, if the SIP trunk or intercluster trunk device receives valid geolocation information from Call Control that differs from previously sent geolocation information, updated geolocation information gets communicated in an UPDATE (SIP trunk) or Notify (intercluster trunk) message.

Incoming Geolocation Change
For SS feature interactions in a remote cluster, the updated geolocation information gets received over an SIP trunk or intercluster trunk in an UPDATE or Notify message.

When such an update is received, the SIP trunk or intercluster trunk parses the PIDF-LO and passes the PIDF-LO to call control and to the LPSession process.
Example PIDF-LO

The following example shows a PIDF-LO that is sent across a SIP trunk. Be aware that the items that are shown in **bold font** are relevant for location conveyance.

```
UPDATE sip:4400@10.10.10.2:5060;transport=tcp SIP/2.0
Date: Sat, 12 Jul 2008 13:28:42 GMT
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated
Geolocation: <cid:4900@10.10.10.1>; inserted-by="10.10.10.1"
Content-ID: 4900@10.10.10.1
Content-Length: 1070
User-Agent: Cisco-CUCM7.1
To: <sip:4400@10.10.10.2>;tag=41258ce2-8620-4005-9aa1-72d99cd54050-16142615
Contact: <sip:4900@10.10.10.1:5060;transport=tcp>
Content-Type: application/pidf+xml
Call-ID: bbb3f390-878b569-47f54c0a010.10.10.2
Via: SIP/2.0/TCP 10.10.10.1:5060; branch=z9h04bnk179f431e3
CSeq: 101 UPDATE
Max-Forwards: 70

<?xml version="1.0" encoding="UTF-8"?>
<pres xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:caps="urn:ietf:params:xml:ns:pidf:caps"
xmlns:cisco="http://www.cisco.com"
entity="pres:geotarget@example.com"
<dm:device id="sg89ae">
<caps:devcaps>
</caps:devcaps>
<gp:geopriv>
<gp:location-info>
<cl:civicAddress>
<cl:country>IN</cl:country>
<cl:A1>KA</cl:A1>
<cl:A2>BLR</cl:A2>
<cl:A3>a3</cl:A3>
<cl:A4>a4</cl:A4>
<cl:A5>a5</cl:A5>
<cl:A6>a6</cl:A6>
<cl:PRD>prd</cl:PRD>
<cl:POD>pod</cl:POD>
<cl:STS>sts</cl:STS>
<cl:HNO>123</cl:HNO>
<cl:HNS>hns</cl:HNS>
<cl:LMK>lmk</cl:LMK>
<cl:LOC>BLDG1</cl:LOC>
<cl:FLR>flr</cl:FLR>
<cl:NAM>nam</cl:NAM>
</cl:civicAddress>
</gp:location-info>
<gp:usage-rules>
<gp:retransmission-allowed>yes</gp:retransmission-allowed>
<gp:retention-expiry>2008-09-03T17:58:19Z</gp:retention-expiry>
</gp:usage-rules>
</gp:geopriv>
<timestamp>2008-09-02T17:58:19Z</timestamp>
</dm:device>
<presence>
```
Location Conveyance Configuration

If geolocation information about devices needs to be communicated across clusters, ensure that location conveyance is configured. To configure location conveyance, follow the steps that Table 24-3 provides.

To associate devices with geolocations, see the “Configuration Checklist for Geolocations” section on page 24-1.

Tip

Before you configure location conveyance, review the “Configuration Checklist for Location Conveyance” section on page 24-4.

Related Topics

- Configuration Checklist for Geolocations, page 24-1
- Configuration Checklist for Geolocation Filters, page 24-3
- Configuration Checklist for Location Conveyance, page 24-4
- Introducing Geolocations, page 24-5
- Overview of Geolocations, page 24-6
- Geolocation Characteristics, page 24-6
- Geolocation Usage for Shared Lines and Route Lists, page 24-8
- Geolocation Identifiers, page 24-8
- Geolocation Interactions, page 24-9
- Geolocation Configuration, page 24-10
- Geolocation Configuration Settings, page 24-12
- Introducing Geolocation Filters, page 24-16
- Geolocation Filter Configuration, page 24-17
- Geolocation Filter Configuration Settings, page 24-20
- Introducing Location Conveyance, page 24-21
- Geolocation Conveyance Across SIP Trunks and Intercluster Trunks, page 24-22
- SIP Trunk Error Handling for Geolocation Information, page 24-22
- Intercluster Trunk Error Handling for Geolocation Information, page 24-23
- Handling a Received Geolocation, page 24-23
- Feature Interactions with Midcall Geolocation Change, page 24-23
- Location Conveyance Configuration, page 24-25
• Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
• Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide
• CTI Route Point Configuration, Cisco Unified Communications Manager Administration Guide
• Gateway Configuration, Cisco Unified Communications Manager Administration Guide
• Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
• Trunk Configuration, Cisco Unified Communications Manager Administration Guide

Additional Cisco Documentation
• Cisco Unified Communications Manager Administration Guide
• Cisco Unified Communications Manager System Guide
• Cisco Unified Serviceability Administration Guide
• Cisco Unified Communications Manager Call Detail Records Administration Guide
• Cisco Unified Real-Time Monitoring Tool Administration Guide
• Cisco Unified Reporting Administration Guide
• Cisco Unified Communications Manager Bulk Administration Guide
• Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager
• Cisco Unified Communications Manager Security Guide
• Cisco Unified Communications Manager Assistant User Guide
Hold Reversion

The hold reversion feature alerts a phone user when a held call exceeds a configured time limit. This chapter provides information on the following topics:

- Configuration Checklist for Hold Reversion, page 25-1
- Introducing Cisco Hold Reversion, page 25-2
- Understanding How Cisco Hold Reversion Works, page 25-3
- System Requirements, page 25-8
- Devices That Support Hold Reversion, page 25-8
- Interactions and Restrictions, page 25-9
- Installing and Activating Cisco Hold Reversion, page 25-11
- Configuring Cisco Hold Reversion, page 25-11
- Configuring Call Focus Priority, page 25-13
- Configuring Hold Reversion Timer Settings, page 25-14
- Providing Cisco Hold Reversion Information to Users, page 25-15
- Troubleshooting Cisco Hold Reversion, page 25-15
- Related Topics, page 25-16

Configuration Checklist for Hold Reversion

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

Table 25-1 shows the steps to configure the hold reversion feature. This procedure assumes that you have configured DNs for phones or are using auto-registration.

- For more information about DN settings and assigning a device pool to a phone, see “Cisco Unified IP Phone Configuration” and “Understanding Directory Numbers” in the Cisco Unified Communications Manager System Guide.

- For more information about device pool settings, see “Device Pool Configuration” in the Cisco Unified Communications Manager Administration Guide.
For more information about settings for Cisco Unified Communications Manager, choose System > Service Parameters, select a server and the Cisco CallManager service, and click the “?” icon at the top of the window.

For related documentation, see “Related Topics” section on page 25-16.

### Table 25-1  Hold Reversion Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If phone users want the hold reversion messages to display in a language other than English, or if you want the user to receive country-specific tones for calls, verify that you installed the locale installer.</td>
</tr>
</tbody>
</table>
| **Step 2**                                                                         | (Optional) Configure the Reverted Call Focus Priority setting in the Device Pool Configuration window for a new or existing device pool. | Configuring Call Focus Priority, page 25-13  
Configuration Tips for Cisco Hold Reversion, page 25-12  
Device Pool Configuration, Cisco Unified Communications Manager Administration Guide |
| **Step 3**                                                                         | In the Service Parameter Configuration window for the Cisco CallManager service, configure the hold reversion timer settings. | Configuring Hold Reversion Timer Settings, page 25-14  
Configuration Tips for Cisco Hold Reversion, page 25-12 |
| **Step 4**                                                                         | In the Phone Configuration window, verify that the correct device pool is configured for the Cisco Unified IP Phone(s). If not, apply the correct device pool. | Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide |
| **Step 5**                                                                         | In the Phone Configuration window, verify that the correct user locale is configured for the Cisco Unified IP Phone(s). | Changing an End User Password, Cisco Unified Communications Manager Administration Guide  
Cisco Unified Communications Operating System Administration Guide |
| **Step 6**                                                                         | Verify that the Cisco CallManager service is activated in Cisco Unified Serviceability. | Cisco Unified Serviceability Administration Guide |

### Introducing Cisco Hold Reversion

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit.

---

**Note**
Throughout this chapter, references to reverted calls apply only to reverted calls that are invoked by the hold reversion feature; these references do not apply to other reverted call types, such as park reverted calls.
As administrator, you can configure hold reversion for any DN that is associated with a phone that is on the same Cisco Unified Communications Manager cluster. The phone device that is associated with the line must support this feature, or hold reversion does not activate. When multiple phone devices share a line, only those devices that support hold reversion can use this feature.

**Note**
Cisco Hold Reversion applies specifically to calls that an end user puts on hold. You cannot activate this feature on calls that the system or network puts on hold; for example, during conference or transfer operations.

The types of alerts that are generated at the phone for reverted calls depend on the capabilities of the phone device. Cisco Unified Communications Manager provides the following alerts when the hold reversion feature activates, depending on the capabilities of the phone and the firmware release that is installed.

- The phone rings once or beeps once.
- The status line briefly displays “Hold Reversion” for the reverted call at the user phone.
- The LED next to the line button flashes continuously on the phone handset, like other alerting operations.
- A “wobbling” handset icon displays for a reverted call.

See the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support hold reversion and this version of Cisco Unified Communications Manager for more information about your phone capabilities.

The following sections provide information on the Cisco Hold Reversion feature:

- Understanding How Cisco Hold Reversion Works, page 25-3
- System Requirements, page 25-8
- Interactions and Restrictions, page 25-9
- Installing and Activating Cisco Hold Reversion, page 25-11
- Configuring Cisco Hold Reversion, page 25-11

**Additional Information**
See the “Related Topics” section on page 25-16.

**Understanding How Cisco Hold Reversion Works**

To enable hold reversion, you configure timer settings for your cluster or for specific phone lines.

- When hold reversion is enabled for the cluster, the hold reversion feature gets invoked when a call that a user at your site puts on hold exceeds the configured time limit, unless the feature is disabled for that line or the phone does not support the hold reversion feature.
- When hold reversion is enabled for a line but not for the cluster, only calls that are received on that line can invoke the hold reversion feature.
- When hold reversion is enabled for both the line and the cluster, the timer settings for the line override the timer settings for the cluster.
The following sections provide detailed operations information:

- Hold Reversion Alerting Operations, page 25-4
- Call Focus Operations, page 25-5
- How to Retrieve Reverted Calls, page 25-5
- Timer Deactivation, page 25-6
- Examples, page 25-6

Additional Information

See the “Related Topics” section on page 25-16.

Hold Reversion Alerting Operations

Table 25-2 provides a summary of hold reversion alerting operations for different call scenarios when hold reversion is invoked for a line or cluster. These operations apply to incoming calls and outgoing calls that a phone user puts on hold.

Hold reversion ring uses the ring settings that are defined in Cisco Unified Communications Manager Administration for that user, except that flash gets converted to flash once and ring gets converted to ring once. If the ring setting specifies disabled, the phone will not ring, flash, or beep.

If the user has another active call, the user also receives call waiting tone once on the reverted call.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Alerting Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming call alerting before hold reversion activates</td>
<td>No hold reversion alerts get sent to the holding phone until the incoming call is answered (except for the hold reversion icon).</td>
</tr>
<tr>
<td>Incoming call alerting after hold reversion activates</td>
<td>No additional alerts get sent to the holding phone until the incoming call is answered.</td>
</tr>
<tr>
<td>Shared line</td>
<td>Only the device that initiates the held call receives alerts. Other instances of the shared line do not receive alerts.</td>
</tr>
<tr>
<td>Multiple reverted calls on the same phone device or on the same phone line with no incoming call</td>
<td>All reverted calls receive alerts. You can configure different alert intervals for different lines.</td>
</tr>
<tr>
<td>Mutual hold</td>
<td>Both parties can receive hold reversion alerts.</td>
</tr>
<tr>
<td>Holding party represents one-sided call; for example, another feature splits the call or redirects the call</td>
<td>Hold reversion alerts get delayed until the holding party reassociates with another party.</td>
</tr>
</tbody>
</table>

Additional Information

See the “Related Topics” section on page 25-16.
Call Focus Operations

A reverted call must have focus, meaning be highlighted on the phone, before it can be retrieved. The call focus priority specifies which call type, incoming calls or reverted calls, has priority for user actions, such as going off hook. At Cisco Unified Communications Manager installation, incoming calls have priority.

You can configure which call type has priority. For example, when incoming calls are configured with a higher priority, if a held call is in the reverted state and the phone goes off hook, Cisco Unified Communications Manager resumes the reverted call only when no incoming call is present.

If the user puts multiple calls on hold for the same line or on the same phone and more than one call is in the reverted state, the oldest call keeps focus, and Cisco Unified Communications Manager resumes the oldest reverted call first, unless an incoming call exists (when incoming calls have priority) or the user chooses to resume another reverted call. Users can choose to retrieve another reverted call by highlighting the call and pressing the Select softkey.

If the phone device of the user has a remote-in-use call and a reverted call, Cisco Unified Communications Manager retrieves the reverted call on off hook.

See the “Call Focus Priority” section on page 25-12 for more information about call focus configuration settings for this feature.

Additional Information
See the “Related Topics” section on page 25-16.

How to Retrieve Reverted Calls

When the reverted call has focus, users can retrieve the reverted call by

- Picking up the handset
- Pressing the speaker button on the phone
- Pressing the headset button
- Selecting the line that is associated with the reverted call
- Pressing the Resume softkey

These actions assume that the handset is idle and the speaker is not already on.

Note
See the Cisco Unified IP Phone user guides for Cisco Unified IP Phone models that support hold reversion and this version of Cisco Unified Communications Manager for more information.

Additional Information
See the “Related Topics” section on page 25-16.
Understanding How Cisco Hold Reversion Works

Timer Deactivation

The hold reversion alerting timers for the hold reversion feature stop when

- The user retrieves a held call.
- The user invokes another feature on the same call.
- The held call gets released.

If the call is not resumed before the clusterwide Maximum Hold Duration Timer system setting expires, Cisco Unified Communications Manager stops the reminder alerts and clears the call. If the Maximum Hold Duration Timer specifies 0, the call remains on hold until the clusterwide Maximum Call Duration Timer setting expires and Cisco Unified Communications Manager clears the call.

See the “Interactions” section for more information about how hold reversion works with Cisco Unified Communications Manager applications and call-processing features.

Additional Information

See the “Related Topics” section on page 25-16.

Examples

The following examples describe how hold reversion works in Cisco Unified Communications Manager:

- Example: Hold Reversion Feature Disabled, page 25-6
- Example: Reverted Call and New Outgoing Call, page 25-6
- Example: Shared Line, page 25-7
- Example: Multiple Reverted Calls on the Same Line, page 25-7
- Example: Multiple Reverted Calls on Different Lines with Incoming Call, page 25-7

In these examples, the hold reversion duration timer, which defines when to activate hold reversion, specifies a setting of 30, and the hold reversion interval timer, which defines when to send reminder alerts, specifies a setting of 20.

Example: Hold Reversion Feature Disabled

User A calls user B, who exists in the same cluster as user A. User B answers the call and puts the call on hold. If MOH is configured for held calls, user A receives music.

Because hold reversion is not enabled for the DN, user B does not receive alerts to indicate that the call remains on hold. The clusterwide Maximum Hold Duration Timer system setting expires, and Cisco Unified Communications Manager clears the call.

Example: Reverted Call and New Outgoing Call

User A calls user B, who exists in the same Cisco Unified Communications Manager cluster as user A. User B answers the call and puts the call on hold. If MOH is configured for held calls, user A receives music.

Cisco Unified Communications Manager notifies user B when the held call assumes the reverted state—after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.)

User B goes off hook to make an outgoing call when the held call is in the reverted state. Cisco Unified Communications Manager resumes the held call. User B cannot make a new outgoing call.
Example: Shared Line

User A and user B exist in the same cluster. User A calls a shared line on user B phone. User B puts the call on hold. If MOH is configured for held calls, user A receives music.

Cisco Unified Communications Manager notifies user B when hold reversion activates for the call—after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.) Other users on the shared line do not receive reverted call alert.

Until user B retrieves the reverted call, Cisco Unified Communications Manager sends periodic reminder alerts every 20 seconds to the holding phone for the DN—Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN at the configured intervals. (Your phone may support additional alerting mechanisms.) No other users on the shared line receive reminder alerts.

User B receives no other calls on the phone. The call has focus, and user B goes off hook. User B retrieves the reverted call.

Note

When the held party is a shared line, other line appearances show normal indicators for a remote-in-use call. When the holding party is a shared line, the remote-in-use indicator does not display on other line appearances after the user puts the call on hold; the remote-in-use indicator redisplayson the other line appearances when the user reconnects with the call. If another user on the shared line picks up the reverted call, the phone of the holding party displays the remote-in-use indicator and no longer displays hold reversion alerts. If the holding party drops off the call, for example, gets released by an application, the hold reversion timers deactivate.

Example: Multiple Reverted Calls on the Same Line

User A and user C call user B on the same DN; user B has Hold Reversion enabled, and call A is a reverted call.

User B answers the call from User C and puts the call on hold. If MOH is configured for held calls, user C receives music.

Cisco Unified Communications Manager notifies user B when call C assumes the reverted state—after 30 seconds, Cisco Unified Communications Manager sends the message “Hold Reversion” to the phone and rings the phone once (or beeps or flashes once) on the holding DN. (Your phone may support additional alerting mechanisms.) User B gets reminder alerts for both calls every 20 seconds.

Call A has focus, and user B retrieves the reverted call from user A.

Example: Multiple Reverted Calls on Different Lines with Incoming Call

User A calls on line B1 for user B, who has hold reversion configured on both B1 and B2. User B puts user A on hold. If MOH is configured for held calls, user A receives music.

User C calls on line B2 for user B. User B puts user C on hold. If MOH is configured for held calls, user C receives music.

Both held calls enter the reverted state when they exceed the preconfigured time limit of 30 seconds. User B gets hold reversion alerts for both held calls.

An incoming call comes in on line B3. Incoming calls have focus priority. User B goes off hook and answers the incoming call. User B ends the B3 call.

Cisco Unified Communications Manager restarts the timer for activating the hold reversion feature on call B1.

**Additional Information**
See the “Related Topics” section on page 25-16.

## System Requirements

Hold reversion requires the following software components:

- Cisco Unified Communications Manager 6.0 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco CTIManager service that is running on at least one server in the cluster
- Cisco Database Layer Monitor service that is running on the same server as the Cisco CallManager service
- Cisco RIS Data Collector service that is running on the same server as the Cisco CallManager service
- Cisco Tftp service that is running on at least one server in the cluster
- Cisco Unified Communications Manager Locale Installer; that is, if you want to use non-English phone locales or country-specific tones (see the [Cisco Unified Communications Operating System Administration Guide](https://www.cisco.com) for information on locale installers)

**Additional Information**
See the “Related Topics” section on page 25-16.

## Devices That Support Hold Reversion

Use the Cisco Unified Reporting application to generate a complete list of devices that support hold reversion. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   - by choosing **File > Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.
5. To generate a report of all devices that support hold reversion, choose these settings from the respective drop-down list boxes and click the Submit button:

- Product: All
- Feature: Hold Reversion

The List Features pane displays a list of all devices that support the hold reversion feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Additional Information
See the “Related Topics” section on page 25-16.

Interactions and Restrictions

The following sections describe the interactions and restrictions for hold reversion:

- Interactions, page 25-9
- Restrictions, page 25-10

Additional Information
See the “Related Topics” section on page 25-16.

Interactions

The following sections describe how hold reversion interacts with Cisco Unified Communications Manager applications and call processing:

- Music on Hold
- Call Park
- MLPP
- CTI Applications

Additional Information
See the “Related Topics” section on page 25-16.

Music on Hold

Cisco Unified Communications Manager supports MOH on a reverted call if MOH is configured for a normal held call.

Call Park

If hold reversion is invoked and the held party presses the Park softkey, the holding party still receives hold reversion alerts and can retrieve the call. When the holding party retrieves the call, the holding party receives MOH, if configured.
If the held party parks before the hold duration exceeds the configured time limit, Cisco Unified Communications Manager suppresses all hold reversion alerts until the call is picked up or redirected.

**MLPP**

When a multilevel precedence and preemption (MLPP) call is put on hold and reverts, the MLPP call loses its preemption status, and the reverted call gets treated as a routine call. After the call reverts, Cisco Unified Communications Manager alerts the user with one ring. Cisco Unified Communications Manager does not play a preemption ring. If a high precedence call becomes a reverted call, Cisco Unified Communications Manager does not play a precedence tone.

**CTI Applications**

CTI applications can access hold reversion functionality when the feature is enabled for a line or the cluster. Cisco-provided applications such as Cisco Unified Communications Manager Assistant and attendant console provide hold reversion functionality using the CTI interface.

When hold reversion gets invoked, the CTI port receives event notification instead of the audible tone presented on Cisco Unified IP Phones. CTI ports and route points receive the event notification once only, whereas Cisco Unified IP Phones receive alerts at regular intervals.

See the following API documents for information about CTI requirements and interactions with hold reversion:

- *Cisco Unified Communications Manager JTAPI Developer Guide*
- *Cisco Unified Communications Manager TAPI Developer Guide*

**Additional Information**

See the “Related Topics” section on page 25-16.

**Restrictions**

The following restrictions apply to the hold reversion feature:

- Cisco Extension Mobility and Cisco Web Dialer features do not support the hold reversion feature.
- This feature does not support SCCP analog phone types, such as ATA 186, DPA-7610, and DPA-7630.
- Only certain on-net phone devices that are running SCCP within a cluster can invoke the hold reversion feature.
- When hold reversion is enabled for the cluster, the phone must have the ability to support the hold reversion feature, or the feature does not activate.
- Shared line devices cannot configure different hold reversion timers.
- Hold reversion ring uses the ring settings that Cisco Unified Communications Manager Administration defines for that user (disable, flash only, ring once, ring, beep only) except that flash gets converted to flash once, and ring gets converted to ring once.
- The maximum number of reverted calls that are allowed on a line equals the maximum number of calls setting for your cluster.
Installing and Activating Cisco Hold Reversion

Hold reversion automatically installs when you install Cisco Unified Communications Manager. After you install Cisco Unified Communications Manager, you must configure hold reversion feature settings in Cisco Unified Communications Manager Administration to enable the feature.

Hold reversion relies on the Cisco CallManager service, so make sure that you activate the Cisco CallManager service in Cisco Unified Serviceability.

Configuring Cisco Hold Reversion

The following sections provide detailed configuration information:

- Hold Reversion Timers in the Service Parameter Window, page 25-12
- Call Focus Priority, page 25-12
- Configuration Tips for Cisco Hold Reversion, page 25-12
- Configuring Call Focus Priority, page 25-13
- Configuring Hold Reversion Timer Settings, page 25-14

Tip

Before you configure hold reversion, review the “Configuration Checklist for Hold Reversion” section on page 25-1.

Additional Information

See the “Related Topics” section on page 25-16.
Chapter 25      Hold Reversion

Hold Reversion Timers in the Service Parameter Window

The following timers in Cisco Unified Communications Manager specify the alert operations for hold reversion:

- The Hold Reversion Duration timer specifies the wait time before a reverted call alert gets issued to the phone of the holding party.
- The Hold Reversion Notification Interval timer specifies the frequency of the periodic reminder alerts to the holding party phone.

For example, a duration timer setting of 20 and an interval setting of 30 means that Cisco Unified Communications Manager will issue the first alert after 20 seconds and a reminder alert every 30 seconds thereafter. The hold reversion feature activates when the hold reversion duration timer times out (after 20 seconds).

See the “Configuring Hold Reversion Timer Settings” section on page 25-14 for the hold reversion timer configuration procedure.

At installation, the value of the hold reversion duration timer settings specifies 0, which means that the feature is disabled. The hold reversion duration line settings remain empty.

Call Focus Priority

When a phone has a reverted call and an incoming call alerting, the call focus priority specifies which call type has focus, meaning which call type has priority for user actions, such as going off hook. At Cisco Unified Communications Manager installation, incoming calls have priority.

As administrator, you configure the Reverted Call Focus Priority setting for a device pool, which you then assign to a phone device in Cisco Unified Communications Manager Administration. The focus priority for the device pool that is associated with the phone applies to reverted and incoming calls that appear on the same line or on different lines on the phone device.

See “Configuring Call Focus Priority” section on page 25-13 for the call focus priority configuration procedure.

Additional Information

See the “Related Topics” section on page 25-16.

Configuration Tips for Cisco Hold Reversion

Consider the following information when you configure the hold reversion feature in Cisco Unified Communications Manager Administration:

- You must set the Hold Reversion Duration timer and Hold Reversion Notification Interval timer settings for your cluster for Cisco CallManager service updates.
- At installation, the Hold Reversion Duration timer specifies 0, which disables the feature.
- You cannot configure hold reversion settings for DNs that are associated with phones that do not support this feature.
- Configure the Maximum Hold Duration Timer system setting to a value greater than 0; otherwise, a reverted call can remain on hold until the Maximum Call Duration Timer expires.
- If you configure the Maximum Hold Duration Timer to a value less than the Hold Reversion Duration timer, the hold reversion feature does not activate.
Chapter 25  Hold Reversion

Configuring Cisco Hold Reversion

• If you leave either the Hold Reversion Ring Duration (seconds) timer setting or Hold Reversion Notification Interval (seconds) timer setting blank in the Directory Number Configuration window, Cisco Unified Communications Manager uses the hold reversion timer settings for the cluster. If you configure a value for either timer in the Directory Number Configuration window, Cisco Unified Communications Manager uses the timer settings for the line.

• If you configure the Hold Reversion Duration timer for either the cluster or a line to a value greater than 0 but do not configure the Hold Reversion Notification Interval timer, Cisco Unified Communications Manager sends just one alert, when the call assumes the reverted state. If you configure the Hold Reversion Notification Interval timer for either the cluster or the line but do not configure Hold Reversion Duration timer to a value greater than 0, the hold reversion feature does not activate.

• Only Cisco Unified IP Phones that support the hold reversion feature display the hold reversion timer settings in the Directory Number Configuration window. If a Cisco Unified IP Phone that supports hold reversion shares a line with a phone device that does not support hold reversion, the hold reversion configuration settings display only for the line on the supporting device.

• If a shared-line device disables this feature, hold reversion gets disabled on all other devices that share that line.

• If the ring settings that are configured for the phone specify Disabled, the phone will not ring, flash, or beep for the hold reversion feature.

• Changing the hold reversion duration timer requires a reset of the device; changing the reverted call priority field requires reset of devices in that device pool.

• To fully disable the hold reversion feature after it is enabled, be sure to disable the Hold Reversion Duration timer on every line in addition to disabling the clusterwide settings.

Additional Information

See the “Related Topics” section on page 25-16.

Configuring Call Focus Priority

Perform the following procedure to configure the call focus priority setting for the hold reversion feature. You can configure this setting in the Default device pool or in another device pool in the list, or you can create a new device pool for hold reversion feature users.

Note

The Not Selected setting specifies the reverted call focus priority setting for the default device pool at installation. At installation, incoming calls have priority. You cannot choose this setting in Cisco Unified Communications Manager Administration.

If you are configuring a new device pool, see “Device Pool Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose System > Device Pool. The Find and List Device Pools window displays.

Step 2  To display the device pools list, click Find, or use the search results from an active query. Choose a device pool in the Find and List Device Pool window.
Configuring Cisco Hold Reversion

Chapter 25      Hold Reversion

Step 3  In the Reverted Call Focus Priority field, choose one of the following settings:
   • Choose **Default** to assign highest priority to incoming calls.
   • Choose **Highest** to assign highest priority to reverted calls.

Step 4  Click the **Save** button.

Step 5  Reset any devices in the device pool to incorporate the change.

---

**Note**  Call focus priority gets sent to the phone that is running SIP by its TFTP configuration file.

---

Additional Information

See the “Related Topics” section on page 25-16.

Configuring Hold Reversion Timer Settings

Perform the following procedure to enable the hold reversion feature and to configure the hold reversion timer settings. This procedure assumes that DNs are configured for a phone or that the phones are using auto-registration.

Consider the following information when you are configuring hold reversion timer settings:

- To enable hold reversion for the cluster, change the Hold Reversion Duration timer in the Service Parameters window to a value greater than 0.
- If you do not want to use the default system setting for reminder alerts, configure the Hold Reversion Notification Interval timer in the Service Parameters window. The default value specifies 30 seconds.
- To disable hold reversion for a line when the system setting is enabled, enter a value of 0 for the Hold Reversion Duration timer in the Directory Number Configuration window. If you leave the field empty, Cisco Unified Communications Manager uses the cluster timer setting.
- To enable hold reversion for a line when the system setting is disabled, set the Hold Reversion Ring Duration (seconds) timer in the Directory Number Configuration window to a value greater than 0. To enable reminder alerts, configure the Hold Reversion Notification Interval timer to a value greater than 0 in the same window or leave it blank to use the cluster setting.
- To configure hold reversion timer settings that differ from the cluster settings when hold reversion is enabled, enter different values for the hold reversion timers in the Directory Number Configuration window.

Procedure

Step 1  Find the hold reversion timers for a line or the cluster:
   • To enable hold reversion and configure timer settings for the cluster, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration.
     - From the Server drop-down list box, choose the server that is running the Cisco CallManager service.
     - From the Service drop-down list box, select the Cisco CallManager service.
   The Service Parameters Configuration window displays. Go to **Step 2**.
• To enable or disable hold reversion and configure hold reversion timer settings for a line, choose **Device > Phone** in Cisco Unified Communications Manager Administration. Click **Find** to display the device pools list, or use the search results from an active query.
  - Choose a device from the phone list that displays in the Find and List Phones window. The Phone Configuration window displays.
  - In the phone configuration window, choose a Directory Number from the list at the left.

The Directory Number Configuration window displays. Go to **Step 2**.

**Step 2** Configure the hold reversion timers:

• In the Hold Reversion Ring Duration (seconds) field, enter a value greater than 0 to enable the hold reversion feature. To disable the hold reversion feature, enter a 0. You can enter a value from 0 to 1200 seconds (inclusive). This timer notifies a user when a held call enters the reverted state.

• If you do not want to use the existing setting for reminder alerts, enter a value between 0 to 1200 seconds (inclusive) in the Hold Reversion Notification Interval (sec) field. Cisco Unified Communications Manager uses this timer to schedule periodic reminder alerts to the phone of the holding party for reverted calls. If you enter a 0, no reminder alerts get sent.

**Step 3** Click the **Save** button.

**Step 4** Reset any devices to incorporate changes in the Directory Number Configuration window.

**Step 5** Repeat this procedure to configure additional timers.

**Additional Steps**
In the Phone Configuration window, verify that the correct device pool is configured for the Cisco Unified IP Phone(s). If not, apply the correct device pool.

**Additional Information**
See the “Related Topics” section on page 25-16.

**Providing Cisco Hold Reversion Information to Users**

The Cisco Unified IP Phone user guides provide procedures for how to use the hold reversion feature. Some Cisco Unified IP Phones have a ? button, which displays help for more information.

**Additional Information**
See the “Related Topics” section on page 25-16.

**Troubleshooting Cisco Hold Reversion**

Use the Cisco Unified Serviceability Trace Configuration and Real Time Monitoring Tool to help troubleshoot hold reversion problems. See the *Cisco Unified Serviceability Administration Guide*.

**Additional Information**
See the “Related Topics” section on page 25-16.
Related Topics

- Configuration Checklist for Hold Reversion, page 25-1
- Introducing Cisco Hold Reversion, page 25-2
- Understanding How Cisco Hold Reversion Works, page 25-3
- System Requirements, page 25-8
- Additional Information, page 25-9
- Interactions and Restrictions, page 25-9
- Installing and Activating Cisco Hold Reversion, page 25-11
- Configuring Cisco Hold Reversion, page 25-11
- Configuring Call Focus Priority, page 25-13
- Configuring Hold Reversion Timer Settings, page 25-14
- Providing Cisco Hold Reversion Information to Users, page 25-15
- Troubleshooting Cisco Hold Reversion, page 25-15
- Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Changing an End User Password, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide

For more information about phones, see the following sections:
- Phone Features, Cisco Unified Communications Manager System Guide
- Cisco Unified IP Phones User Guides and Administration Guides for phone models that support hold reversion and this release of Cisco Unified Communications Manager

Additional Cisco Documentation

- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager System Guide
- Cisco Unified Serviceability Administration Guide
Hotline

The hotline feature extends the Private Line Automatic Ringdown (PLAR) feature, which allows you to configure a phone so that when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The hotline feature adds the additional restriction that hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers.

Hotline phones typically have a restricted feature set. You can restrict the features on a hotline phone by applying a softkey template to the phone. You can configure a hotline phone to originate calls only, terminate calls only, or originate and terminate calls.

Hotline uses route class signalling to allow hotline phones to receive calls only from other hotline phones. Hotline also provides configurable call screening based on caller ID, which allows a receiving hotline phone to screen calls and allow only callers in the screening list to connect.

This chapter, which provides information on the hotline feature for Cisco Unified Communications Manager, contains the following topics:

- Configuration Checklist for Hotline, page 26-1
- Introducing Hotline for Cisco Unified Communications Manager, page 26-3
- System Requirements for Hotline, page 26-6
- Installing and Activating Hotline, page 26-7
- Configuring Hotline, page 26-7
- Troubleshooting Hotline, page 26-12
- Related Topics, page 26-12

Configuration Checklist for Hotline

The hotline feature extends the Private Line Automatic Ringdown (PLAR) feature, which allows you to configure a phone so that when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The hotline feature adds the additional restriction that hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers.

Hotline phones typically have a restricted feature set. You can restrict the features on a hotline phone by applying a softkey template to the phone. You can configure a hotline phone to originate calls only, terminate calls only, or originate and terminate calls.
Hotline uses route class signalling to allow hotline phones to receive calls only from other hotline phones. Hotline also provides configurable call screening based on caller ID, which allows a receiving hotline phone to screen calls and allow only callers in the screening list to connect.

Table 26-1 provides a checklist for configuring hotline in your network. Use Table 26-1 in conjunction with the “Related Topics” section on page 26-12.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure hotline service parameters.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure PLAR, which makes a phone dial a preset number when it goes offhook.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Check the <strong>Hotline Device</strong> check box in the Phone Configuration window.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure translation patterns or route patterns to assign a route class to inbound T1 CAS calls and strip off the corresponding prefix digit.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure the call and receive settings for the phone. This is only necessary if you want to restrict a hotline phone to only originating calls or only terminating calls.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Create a softkey template that blocks unwanted features and apply it to the phone.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Introducing Hotline for Cisco Unified Communications Manager

The hotline feature extends the Private Line Automatic Ringdown (PLAR) feature, which allows you to configure a phone so that when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from a phone that gets configured for PLAR. Hotline adds the following additional restrictions and administrator controls for phones that use PLAR:

- Hotline devices (devices configured to use hotline) that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers
- You can configure a hotline phone to call only, receive only, or both call and receive.

---

**Table 26-1 Hotline Configuration Checklist (continued)***

<table>
<thead>
<tr>
<th>Configuration Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
</tr>
</tbody>
</table>
Introducing Hotline for Cisco Unified Communications Manager

You can restrict the features available on a hotline phone by applying a softkey template to the phone.

Analog hotline phones ignore inbound hookflash signals.

**Route Class Signalling**
A route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. A hotline phone can only accept calls with the same route class from a hotline phone.

You set the route class of a call by configuring route patterns or translation patterns.

**Configurable Call Screening**
Configurable Call Screening allows a receiving hotline phone to screen calls based on caller ID information and allow only callers in a screening list to connect.

You configure the call screen setting on translation patterns.

More information about the hotline feature is available in the following sections:

- Configuring Phone Call and Receive Settings, page 26-4
- Configuring Call Screening, page 26-4

### Configuring Phone Call and Receive Settings

You can configure a hotline phone to call only, receive only, or both call and receive. You configure this by using Calling Search Spaces (CSS) and partitions, as described in this example:

1. Create a CSS named NoRouteCSS, and two partitions named EmptyPartition and IsolatedPartition.
2. Do not assign the EmptyPartition partition to any line.
3. Configure the NoRouteCSS CSS to select only the EmptyPartition partition.
4. Do not select the IsolatedPartition partition on any CSS window.
5. To receive only, assign the NoRouteCSS CSS to the phone.
6. To call only, assign the IsolatedPartition partition to the phone.

### Configuring Call Screening

You can screen calls to a terminating hotline phone such that only callers in a screening list are allowed to connect. You typically use this feature to allow a terminating hotline to receive calls from more than one originator (pair-protected) but less than every originator in the same class (non-pair protected). The following sections describe the two methods to implement caller screening:

- Configuring Call Screening With Calling Search Spaces and Partitions, page 26-4
- Configuring Call Screening With Calling Party Number Routing, page 26-5

### Configuring Call Screening With Calling Search Spaces and Partitions

For all intraswitched (line to line) hotline calls, you can configure call screening by managing the Calling Search Space (CSS) and partition configuration, as described in the following example:

1. Assign the terminating line to a partition to protect it.
2. Create the screening list by including the terminating partition in only the CSSs of originating hotline phones that you want to allow to connect to the terminating hotline.

### Configuring Call Screening With Calling Party Number Routing

Because trunks are associated with more than one inbound/outbound phone, the CSS and partition method of call screening described in the “Configuring Call Screening With Calling Search Spaces and Partitions” section on page 26-4 cannot be used to build per-DN screens. Cisco Unified Communications Manager can use the Calling Party Number to make routing decisions.

This call screening method can also be used for lines, but it is particularly useful for connection paths involving trunks such as the following:

Phone - PBX - Gateway - Cisco Unified Communications Manager - Gateway - PBX - Phone

If you cannot screen at the PBX, then this method allows you to screen for the PBX by using Cisco Unified Communications Manager.

Figure 26-1 on page 26-5 and the description that follows illustrate this method.

- InboundDevice_C is the inbound CSS for the trunk or line on which the call came in.
- InboundDevice_P is a partition that is a member of InboundDevice_C.
XP(BobsDN) is a translation pattern that is a member of InboundDevice_P, which directs all calls to Bob's DN to go through Bob's screener. The check box Route Next Hop By Calling Party is checked in the translation pattern window. The CSS for the next hop is set to BobsScreener_C.

For inbound PLAR lines, this pattern would match on blank and transform the blank called party to Bob's DN.

XP(*) is a wildcard translation pattern for all inbound calls whose destination has no associated screen.

BobsScreener_C and BobsScreener_P are the CSS and Partition, respectively, to hold calling party number screening patterns for Bob.

XP(AlicesDN) is a translation pattern belonging to BobsScreener_P, representing a calling party (Alice) that needs to be allowed to connect. For these patterns, the CSS should be set to OutboundDevice_C.

OutboundDevice_C, OutboundDevice_P, and DN(cdpnXxxx) or RP(cdpnXxxx) are all normal dial plan configurations to go out lines and trunks.

Either the DN or the route pattern are part of the partition, but not both.

To build a screening list, create one translation pattern for each pattern that you want to allow through.

### System Requirements for Hotline

The following hotline system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager 8.0(1) or higher on each server in the cluster
- MGCP gateway POTS phones (FXS).
- SCCP gateway POTS phones (FXS).

---

**Tip**

Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). You do not need a Cisco.com account to access Cisco Feature Navigator.

### Devices That Support Hotline

Use the Cisco Unified Reporting application to generate a complete list of devices that support hotline. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.

   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.
2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all devices that support hotline, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Hotline

   The List Features pane displays a list of all devices that support the hotline feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*, which you can find at this URL:


### Installing and Activating Hotline

After you install Cisco Unified Communications Manager, your network can support hotline if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for Hotline” section on page 26-1.

### Configuring Hotline

This section contains information on the following topics:

- Configuring Service Parameters for Hotline, page 26-7
- Accessing Hotline Configuration Settings in Cisco Unified Communications Manager Administration, page 26-9

**Tip**

Before you configure hotline, review the “Configuration Checklist for Hotline” section on page 26-1.

### Configuring Service Parameters for Hotline

Table 26-2 describes the service parameters that you can configure for hotline. To configure service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**.

All of these service parameters support the Cisco Unified Communications Manager service.

**Tip**

For a step-by-step procedure on how to configure enterprise parameters, see the “Enterprise Parameter Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*. For a step-by-step procedure on how to configure service parameters, see the “Service Parameter Configuration” in the *Cisco Unified Communications Manager Administration Guide*. 
### Table 26-2  Enterprise and Service Parameters for Hotline

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Class Trunk Signaling Enabled</td>
<td>This parameter determines whether Cisco Unified Communications Manager processes (inbound) and sends (outbound) route class signaling on trunks that support it. Route class trunk signaling enables interworking between IP and TDM switches that use route class. Set it to True to enable route class trunk signaling, or to False to disable it. This field is required. The default equals True.</td>
</tr>
</tbody>
</table>
| SIP Satellite Avoidance Route Class Label | This parameter specifies a label representing the Satellite Avoidance route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP satellite avoidance route class value. This label proves useful when interworking with TDM networks that make routing decisions based on satellite avoidance route class. You can change this parameter based on your own vendor-specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter. The following rules apply to values that you specify for this parameter:  
  - Maximum of 64 characters.  
  - Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed.  
  - Dashes are only allowed between alphanumeric characters.  
  This field is required and hidden. The default equals nosat.  
The hotline feature does not use this parameter. It supports other route class features. |
| SIP Hotline Voice Route Class Label    | This parameter specifies a label representing the Hotline Voice route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP Hotline Voice route class value. This label proves useful when interworking with TDM networks that make routing decisions based on Hotline Voice route class. You can change this parameter based on your own vendor-specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter. The following rules apply to values that you specify for this parameter:  
  - Maximum of 64 characters.  
  - Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed.  
  - Dashes are only allowed between alphanumeric characters.  
  This field is required. The default equals hotline. |
Chapter 26      Hotline

Configuring Hotline

Table 26-3  describes the hotline configuration settings in Cisco Unified Communications Manager Administration, except for hotline service parameters, which are described in Table 26-2. For related configuration procedures, see the following sections:

- Configuring Service Parameters for Hotline, page 26-7
- Configuring a Trunk, Cisco Unified Communications Manager Administration Guide

Table 26-2    Enterprise and Service Parameters for Hotline (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Hotline Data Route Class Label</td>
<td>This parameter specifies a label representing the Hotline Data route class in SIP signaling, as defined by the owner of the domain name specified in the SIP Route Class Naming Authority service parameter. Cisco Unified Communications Manager combines the value in this parameter with the value in the SIP Route Class Naming Authority parameter to create the complete signaling syntax for the SIP Hotline Data route class value. This label proves useful when interworking with TDM networks that make routing decisions based on Hotline Data route class. You can change this parameter based on your own vendor-specific or deployment-specific requirements. Make certain that the far-end switch expects to receive the same value that you configure in this parameter. See the help text for the service parameter SIP Route Class Naming Authority for additional information pertinent to this parameter.</td>
</tr>
<tr>
<td></td>
<td>- The following rules apply to values that you specify for this parameter:</td>
</tr>
<tr>
<td></td>
<td>- Maximum of 64 characters.</td>
</tr>
<tr>
<td></td>
<td>- Only alphanumeric (A-Z, a-z,0-9) or dash (-) characters are allowed.</td>
</tr>
<tr>
<td></td>
<td>- Dashes are only allowed between alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>This field is required. The default equals <strong>hotline-ccdata</strong>.</td>
</tr>
</tbody>
</table>

Accessing Hotline Configuration Settings in Cisco Unified Communications Manager Administration

Table 26-3  Hotline Settings in Cisco Unified Communications Manager Administration

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device &gt; Phone</td>
<td>Check this check box to make this device a hotline device. Hotline devices that receive calls will only receive calls from other hotline devices, and will reject non-hotline callers. This feature is an extension of PLAR, which configures a phone to automatically dial one directory number when it goes off-hook. Hotline provides additional restrictions that you can apply to devices that use PLAR. To implement hotline, you must also create a softkey template without supplementary service softkeys, and apply it to the hotline device.</td>
</tr>
</tbody>
</table>

Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communications Manager
Chapter 26      Hotline

Configuring Hotline

Device > Trunk

Route Class Signaling Enabled

From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values:

- **Default**—If you choose this value, the device uses the setting from the Route Class Signaling service parameter.
- **Off**—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter.
- **On**—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter.

Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature.

This parameter is available on SIP trunks.

Device > Gateway

Route Class Signaling Enabled

From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values:

- **Default**—If you choose this value, the device uses the setting from the Route Class Signaling service parameter.
- **Off**—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter.
- **On**—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter.

Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature.

This parameter is available on MGCP PRI and T1/CAS gateway ports.

Encode Voice Route Class

Check this check box to encode voice route class for voice calls. Because voice is the default route class, it typically does not need explicit encoding. If this is disabled (the default setting), the port will not explicitly encode the voice route class. The voice route class (explicitly encoded or not) can get used by downstream devices to identify a call as voice.

This parameter is available on MGCP T1/CAS gateway ports.

Table 26-3 Hotline Settings in Cisco Unified Communications Manager Administration (continued)

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device &gt; Trunk</strong></td>
<td></td>
</tr>
<tr>
<td>Route Class Signaling</td>
<td>From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values:</td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>—If you choose this value, the device uses the setting from the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong>—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong>—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature.</td>
</tr>
<tr>
<td></td>
<td>This parameter is available on SIP trunks.</td>
</tr>
<tr>
<td><strong>Device &gt; Gateway</strong></td>
<td></td>
</tr>
<tr>
<td>Route Class Signaling</td>
<td>From the drop-down list, enable or disable route class signaling for the port. Choose one of the following values:</td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong>—If you choose this value, the device uses the setting from the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong>—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong>—Choose this value to disable route class signaling. This setting overrides the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the hotline feature.</td>
</tr>
<tr>
<td></td>
<td>This parameter is available on MGCP PRI and T1/CAS gateway ports.</td>
</tr>
<tr>
<td>Encode Voice Route</td>
<td>Check this check box to encode voice route class for voice calls. Because voice is the default route class, it typically does not need explicit encoding. If this is disabled (the default setting), the port will not explicitly encode the voice route class. The voice route class (explicitly encoded or not) can get used by downstream devices to identify a call as voice.</td>
</tr>
<tr>
<td>Class</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This parameter is available on MGCP T1/CAS gateway ports</td>
</tr>
</tbody>
</table>
Configuring Hotline

Call Routing > Route/Hunt > Route Pattern

Route Class
Choose a route class setting for this route pattern from the drop-down list box:
- Default
- Voice
- Data
- Satellite Avoidance
- Hotline voice
- Hotline data

The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call.

You should only use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration.

Call Routing > Translation Pattern

Route Class
Choose a route class setting for this translation pattern from the drop-down list box:
- Default
- Voice
- Data
- Satellite Avoidance
- Hotline voice
- Hotline data

The route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. The Default setting uses the existing route class of the incoming call.

You should only use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration.

Route Next Hop By Calling Party Number
Check this box to enable routing based on the calling party number, which is required for call screening based on caller ID information to work between clusters.
Troubleshooting Hotline

For hotline troubleshooting information, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Related Topics

- Configuration Checklist for Hotline, page 26-1
- Introducing Hotline for Cisco Unified Communications Manager, page 26-3
- System Requirements for Hotline, page 26-6
- Installing and Activating Hotline, page 26-7
- Configuring Hotline, page 26-7
- Troubleshooting Hotline, page 26-12

Table 26-3

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device &gt; Device Settings &gt; Softkey Template</td>
<td>To configure SoftKey Templates that remove supplementary service softkeys from hotline phones.</td>
</tr>
</tbody>
</table>
Immediate Divert

The Immediate Divert (iDivert) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls. This chapter provides the following information about immediate divert:

- Configuration Checklist for Immediate Divert, page 27-1
- Introducing Immediate Divert, page 27-2
- System Requirements for Immediate Divert, page 27-3
- Immediate Divert Scenarios With Use Legacy Immediate Divert Service Parameter Set to False, page 27-7
- Installing and Activating Immediate Divert, page 27-10
- Configuring Immediate Divert, page 27-10
- Setting the Service Parameters for Immediate Divert, page 27-10
- Related Topics, page 27-11

Configuration Checklist for Immediate Divert

The Immediate Divert (iDivert) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Table 27-1 provides a checklist to configure immediate divert. For more information on immediate divert, see the “Introducing Immediate Divert” section on page 27-2 and the “Related Topics” section on page 27-11.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Change the Call Park Display Timer clusterwide service parameter if the default is not appropriate.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Change the Use Legacy Immediate Divert clusterwide service parameter if the default is not appropriate.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Change the Allow QSIG During iDivert clusterwide service parameter if the default is not appropriate.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Change the iDivert User Response Timer service parameter if the default is not appropriate.</td>
</tr>
</tbody>
</table>
Introducing Immediate Divert

The Immediate Divert (iDivert or Divert softkeys) feature allows you to immediately divert a call to a voice-messaging system. When the call gets diverted, the line becomes available to make or receive new calls.

Although the immediate divert feature is not available to CTI applications, a CTI redirect operation exists that performs the same function as immediate divert. Application developers can use the CTI redirect operation to accomplish immediate divert.

Access the Immediate Divert feature by using the iDivert or Divert softkey. Configure this softkey by using the Softkey Template Configuration window of Cisco Unified Communications Manager Administration. The softkey template gets assigned to phones that are in the Cisco Unified Communications Manager system.

Consider immediate divert, a Cisco Unified Communications Manager supplementary service, as available for general use within the system. Immediate divert does not require the user to log in to make the iDivert or Divert softkey available on the phone.
You can divert inbound calls that are in the call offering, call on hold, or call active states. You can divert outbound calls in the call active or call hold states. The diverted party receives the greeting of the voice-messaging system of the party to whom the call gets diverted.

Legacy iDivert allows diversion of a call to the voice mailbox of the party that invokes the iDivert feature. Enhanced iDivert allows diversion of a call to either the voice mailbox of the party that invokes the iDivert feature or to the voice mailbox of the original called party.

When enhanced iDivert mode is active for incoming calls, the user to whom a call is presented can invoke immediate divert to divert the call either to the voice mailbox of the user or to the voice mailbox of the original called party. After the invoking user presses the iDivert softkey, a screen on the invoking user phone identifies both the original called party and the invoking user. The user selects one of the two names, and the call gets redirected to the voice mailbox of the selected party.

**Note**

When users invoke the Immediate Divert feature to divert an incoming call, they receive the choice of the original called party only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. See the “Setting the Service Parameters for Immediate Divert” section on page 27-10.

---

### System Requirements for Immediate Divert

Immediate divert requires the following software component to operate:

- Cisco Unified Communications Manager 6.0 or later
- Table 27-2 lists the phones that use the Divert or iDivert softkey

#### Table 27-2 Cisco Unified IP Phones That Use iDivert or Divert Softkeys

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Divert Softkey</th>
<th>iDivert Softkey</th>
<th>What to configure in softkey template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6900 Series (except 6901 and 6911)</td>
<td>X</td>
<td></td>
<td>iDivert</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7900 Series</td>
<td></td>
<td>X</td>
<td>iDivert</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 8900 Series</td>
<td>X</td>
<td></td>
<td>Configured by default</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 9900 Series</td>
<td>X</td>
<td></td>
<td>Configured by default</td>
</tr>
</tbody>
</table>

To find more information about Cisco Unified IP Phones and the Immediate Divert feature, see the phone user documentation at the following sites:


The following voice-messaging systems support immediate divert:

- Voice-messaging systems such as Unity that use the skinny protocol
- Voice-messaging systems such as Octel that use SMDI
Call-Processing Requirements for Immediate Divert

The following sections describe call-processing requirements for immediate divert:

- Softkey Requirements, page 27-4
- Requirements for Incoming Calls, page 27-4
- Requirements for Outgoing Calls, page 27-5

Softkey Requirements

Because the iDivert softkey does not automatically get configured in a softkey template, use the Softkey Template Configuration window in Cisco Unified Communications Manager Administration to configure the iDivert softkey in any available softkey template. You can configure the iDivert softkey in the following call states:

- Connected
- On hold
- Ring in

Note: The ring-in state in the softkey template represents the call-offering state in the phone call state.

Use the Phone Configuration window in Cisco Unified Communications Manager Administration to assign the softkey template that contains the iDivert softkey to a phone.

For information about softkey template configuration, see Softkey Template Configuration in the Cisco Unified Communications Manager Administration Guide. For information about assigning softkey templates to phones, see Cisco Unified IP Phone Configuration in the Cisco Unified Communications Manager Administration Guide.

Requirements for Incoming Calls

The following list gives called party types in the call-forwarding chain that immediate divert supports:

- Party A calls party B.
- Party B forwards to party C.
- Party C forwards to party D.

Party B represents the original called party. Party C represents the last redirecting party. Party D represents the last called party.

Immediate divert supports the following incoming call states:

- Call offering
- Call on hold
- Call active

When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to True, immediate divert redirects the incoming call to the voice-messaging mailbox that is associated with the called party. You can administer a voice-messaging mailbox for the called party through the voice-messaging profile that is assigned to the directory number of the called party.
When the called party presses the iDivert softkey and the Use Legacy Immediate Divert clusterwide service parameter is set to False, immediate divert may allow the called party to select the destination voice mailbox. A screen gets presented to the called party if the call had previously diverted (see the “Interactions” section on page 27-8). The called party can choose to divert the call to the voice-messaging mailbox of the original called party or to the voice-messaging mailbox that is associated with the called party, or the called party can cancel the divert that is in the iDivert menu. You may administer a voice-messaging mailbox for the original called party or for the called party through the voice-messaging profile that is assigned to the associated directory numbers.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the Cisco Unified Communications Manager Administration Guide, and Voice Mail Connectivity to Cisco Unified Communications Manager in the Cisco Unified Communications Manager System Guide.

### Requirements for Outgoing Calls

Immediate divert supports the following outgoing call states:

- Call on hold
- Call active

When the calling party presses the iDivert softkey, immediate divert redirects an outgoing call to the voice-messaging mailbox that is associated with the calling party. You may administer a voice-messaging mailbox for the calling party through the voice-messaging profile that is assigned to the directory number of the calling party.

For information about voice messaging, see Cisco Voice-Mail Pilot Configuration and Voice-Mail Profile Configuration in the Cisco Unified Communications Manager Administration Guide, and Voice Mail Connectivity to Cisco Unified Communications Manager in the Cisco Unified Communications Manager System Guide.

### Immediate Divert Phone Display Messages

Immediate divert displays the following messages on the IP phone to indicate the status of an immediate divert action:

- Key is not active—The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.
- Temporary failure—The voice-messaging system does not work, or a network problem exists.
- Busy—This message indicates that a voice-messaging system is busy.

### Using Immediate Divert

The following scenarios provide examples of using the Immediate Divert feature. Scenario 1 through scenario 6 assume that the Use Legacy Immediate Divert clusterwide service parameter is set to True. Scenario 7 through scenario 8 assume that the Use Legacy Immediate Divert clusterwide service parameter is set to False. Scenario 9 assumes the Use Legacy Immediate Divert clusterwide service parameter is set to False and the Auto Call Pickup Enabled clusterwide service parameter is set to False. All scenarios describe the iDivert softkey, but the Divert softkey is also applicable in these examples (see Table 27-2).
Immediate Divert Scenarios with Use Legacy Immediate Divert Service Parameter Set to True

Scenario 1: Called Party Presses iDivert Softkey
1. Party A calls Manager A.
2. Manager A presses the iDivert softkey (call-offering state).
3. Immediate divert diverts the call to Manager A voice-messaging mailbox.
4. Party A receives the voice-messaging mailbox greeting of Manager A.

Scenario 2: Voice-Messaging Profile of an Original Called Party Does Not Have Voice-Messaging Pilot
1. Party A calls Party B.
2. The call gets forwarded to the personal line of Assistant B.
3. Assistant B presses the iDivert softkey (call-offering state).
4. Immediate divert diverts the call to Assistant B voice-messaging mailbox. Party B does not have a voice-messaging pilot number that is configured, but Assistant B does.
5. Party A receives the voice-messaging mailbox greeting of Assistant B.

Scenario 3: Manager A Forwards a Call to Manager B
1. Party A calls Manager A.
2. Manager A has line forwarded to Manager B.
3. Manager B presses the iDivert softkey (call-offering state).
4. Immediate divert diverts the call to Manager B voice-messaging mailbox.
5. Party A receives the voice-messaging mailbox greeting of Manager B.

Scenario 4: Voice-Messaging Port That Is Defined in a Voice-Messaging Profile is Busy
1. Party A calls Party B.
2. Party B presses the iDivert softkey (call offering state).
3. Immediate divert cannot divert the call to the voice-messaging mailbox because the voice-messaging port is busy.
4. Party B sees the message Busy on the IP phone.
5. The original call remains in the call-offering state.

Scenario 5: Calling Party Calls a Call Center That Uses a Hunt Pilot Number
1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state), which is greyed out.
3. Immediate divert cannot divert the call to the voice-messaging mailbox because Hunt List A does not have a voice-messaging profile.
4. Hunt List A member sees the Key is Not Active message on the IP phone.

Scenario 6: Calling Party B Transfers a Call to Party C on Different Cisco Unified Communications Manager Cluster
1. Party A calls Party B.
2. Party B transfers the call to Party C on a different Cisco Unified Communications Manager cluster.
3. Party C answers the incoming call.
4. Party C presses the iDivert softkey.
5. Party A receives the voice-messaging mailbox greeting of Party C.

Immediate Divert Scenarios With Use Legacy Immediate Divert Service Parameter Set to False

Scenario 7: Calling Party A Calls Party B, and Party B Forwards the Call to Party C
1. Party A calls Party B.
2. Party B phone forwards the call to Party C.
3. Party C gets presented with the incoming call and presses the iDivert softkey.
4. Party C presses the iDivert softkey.
5. Party C receives a screen that offers the choice of diverting to Party B voice-messaging mailbox or Party C voice-messaging mailbox.
6. Party C chooses the voice-messaging mailbox of Party B.
7. Party A receives the voice-messaging mailbox greeting of Party B.

Scenario 8: Calling Party Calls a Call Center That Uses a Hunt Pilot Number
1. Party A calls Hunt List A.
2. Hunt List A member presses the iDivert softkey (call offering state).
3. Immediate divert diverts the call to the voice-messaging mailbox of the hunt list A member that invokes the iDivert feature.
4. Party A receives the voice-messaging mailbox greeting of Hunt List A member.

Scenario 9: Auto Call Pickup Enabled Clusterwide Service Parameter is Set to False, and a User is in a Call Pickup Group
2. Party A calls Party B.
3. Party B IP phone rings but Party B does not answer the call.
4. Party C uses call pickup to answer the call.
5. If Party C presses the iDivert softkey during alerting state, connected state, or on hold state, the IP phone display gets presented to Party C. Party C can choose between two options: iDivert the call to the original called party voice-messaging mailbox (Party B) or iDivert the call to the last called party voice-messaging mailbox (Party C).

Note
If the Use Legacy Immediate Divert clusterwide service parameter is set to False, and the Auto Call Pickup Enabled clusterwide service parameter is set to True, and a user of a call pickup group uses call pickup to answer a call, the IP phone display will not present any choices to the user when the iDivert softkey is pressed.

Interactions and Restrictions

The following sections describe the interactions and restrictions for immediate divert:

- Interactions, page 27-8
Interactions

The following sections describe how immediate divert interacts with Cisco Unified Communications Manager applications and call processing:

- Multilevel Precedence and Preemption (MLPP), page 27-8
- Setting the Service Parameters for Call Park, page 5-11
- Call Forward, page 27-8
- Call Detail Records (CDR), page 27-8
- Conference, page 27-8
- Hunt List, page 27-8

Multilevel Precedence and Preemption (MLPP)

The following interactions occur between immediate divert and MLPP:

- Immediate divert diverts calls to voice-messaging mailboxes regardless of the type of call (for example, a precedence call).
- When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) gets deactivated.

Call Forward

When the Forward No Answer setting on the Directory Number Configuration window is not configured, call forward uses the clusterwide CFNA timer service parameter, Forward No Answer Timer. If a user presses the iDivert softkey at the same time as the call is being forwarded, the call gets diverted to an assigned call forward directory number (because the timer was too short), not the voice-messaging mailbox. To solve this situation, set the CFNA timer service parameter to enough time (for example, 60 seconds). If the iDivert screen has been presented to the iDivert invoker and the CFNA timer expires, the call forwards onward.

Call Detail Records (CDR)

Immediate divert uses the immediate divert code number in the Onbehalf of fields (for example, joinOnbehalfOf and lastRedirectRedirectOnBehalfOf) in CDR.

Conference

When a conference participant presses the iDivert softkey, the remaining conference participants receive the voice-messaging mailbox greeting of the immediate divert initiator. Conference types include Ad Hoc, Meet-Me, Barge, cBarge, and Join.

Hunt List

Immediate divert works as follows for DNs that are members of a line group:
Interactions and Restrictions

• Ensure the iDivert softkey is enabled

• For calls that reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey will appear grayed out if the Use Legacy Immediate Divert clusterwide service parameter is set to True; otherwise, it does not appear grayed out.

• For calls that do not reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey does not appear grayed when the Use Legacy Immediate Divert clusterwide service parameter is set to True or False. (This includes scenarios where a call was made to a hunt list pilot, the hunt list was exhausted, and the call followed the forwarding disposition to the DN that also happens to be a member of a hunt group. This would represent a case where a call reaches a member of a hunt group indirectly through a hunt list pilot.)

Restrictions

The following restrictions apply to immediate divert:

• Immediate divert supports QSIG devices (QSIG-enabled H-323 devices, MGCP PRI QSIG T1 gateways, and MGCP PRI QSIG E1 gateways), depending on the setting of the Use Legacy Immediate Divert and Allow QSIG During iDivert clusterwide service parameters. See the “Setting the Service Parameters for Immediate Divert” section on page 27-10 for details. When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice-mail profile that includes either a voice mail pilot or a voice mail mask or both should leave the “Make this the default Voice Mail Profile for the System” check box unchecked. Ensure the default Voice Mail Profile setting is always set to No Voice Mail.

• When Call Forward All (CFA) and Call Forward Busy (CFB) are activated, the system does not support immediate divert (CFA and CFB have precedence over immediate divert).

• When it reaches a voice-messaging system over a local/SCCP connection, iDivert can detect a busy condition on the voice-messaging ports. (The call cannot divert to a busy voice-messaging system, but the original call gets maintained. Busy will display on the phone on which iDivert was invoked to indicate that the call was not diverted.) When a voice-messaging system is reached over a QSIG or SIP trunk, iDivert can be detected, but the call does not get maintained. When the Allow QSIG During iDivert clusterwide service parameter is set to True, or the Use Legacy Immediate Divert clusterwide service parameter is set to False, immediate divert supports access to voice-messaging systems that can be reached over QSIG/SIP trunks. When the Allow QSIG During iDivert clusterwide service parameter is set to False, and the Use Legacy Immediate Divert clusterwide service parameter is set to True, immediate divert does not support access to voice-messaging systems over QSIG or SIP trunks. Immediate divert cannot divert a call to a busy voice-messaging port; however, voice-messaging ports can exist as members of a route/hunt list, thus reducing the busy port scenario.

• If the Use Legacy Immediate Divert clusterwide service parameter is set to True, members of a hunt list can invoke iDivert if the call is direct. They cannot invoke iDivert if they are reached as a member of a line group. The message, Key is Not Active, displays on the IP phone.

• When Cisco Unified Communications Manager goes down, users cannot leave voice messages unless a media path was established between a redirected party and the voice-messaging system before the Cisco Unified Communications Manager went down.

• System does not support using Malicious Caller ID and Immediate Divert features together.

• CTI applications do not have immediate divert available (applications use Transfer to Voicemail).

• Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also gets changed.
• See the “Multilevel Precedence and Preemption (MLPP)” section on page 27-8 for restrictions about using MLPP.

• A race condition in connection with the Forward No Answer Timeout exists when the iDivert softkey gets pressed. For example, if a manager presses the iDivert softkey immediately after the Forward No Answer timeout, call forward forwards the call to a preconfigured directory number. However, if the manager presses the iDivert softkey before the Forward No Answer timeout, immediate divert diverts the call to the voice-messaging mailbox of the manager.

• The calling and called parties can divert the call to their voice-messaging mailboxes if both simultaneously press the iDivert softkey. The voice-messaging mailbox of the calling party would contain a portion of the outgoing greeting of the called party. Similarly, the voice-messaging mailbox of the called party would contain a portion of the outgoing greeting of the calling party.

• When one participant in a conference presses the iDivert softkey, all remaining participants receive an outgoing greeting of the participant who pressed iDivert. Conference types include Meet-Me, Ad Hoc, cBarge, and Join.

• If the last action on a call was Auto Pickup, Call Transfer, Call Park, Call Park Reversion, Conference, Meet-Me Conference, or any application that performs a split or join operation, enhanced iDivert does not present a screen to a called party to choose the voice-messaging mailbox. Instead, enhanced iDivert immediately diverts the call to the voice-messaging mailbox that is associated with the called party.

• When iDivert is allowed over QSIG trunks, follow these guidelines: when you use QSIG integration with your voice-messaging system, a voice mail profile that includes either a voice mail pilot or a voice mail mask or both should leave the “Make this the default Voice Mail Profile for the System” check box unchecked. Ensure the default Voice Mail Profile setting always gets set to No Voice Mail.

### Installing and Activating Immediate Divert

Immediate Divert, a system feature, comes standard with Cisco Unified Communications Manager software. Immediate divert does not require special installation.

### Configuring Immediate Divert

This section contains the following information:

- Configuration Checklist for Immediate Divert, page 27-1
- Setting the Service Parameters for Immediate Divert, page 27-10

Before you configure immediate divert, review the “Configuration Checklist for Immediate Divert” section on page 27-1.

### Setting the Service Parameters for Immediate Divert

The behavior of the Immediate Divert feature depends on the setting for various service parameters. Descriptions of the service parameters that affect the Immediate Divert feature follow.
Call Park Display Timer Clusterwide Service Parameter

Immediate divert uses the Cisco Unified Communications Manager clusterwide service parameter Call Park Display Timer. The default for this service parameter specifies 10 seconds. Use the Call Park Display Timer service parameter to control the timer for the immediate divert text display on the IP phones. When the service parameter gets changed, the text display timer for immediate divert also changes. Set this timer for each server in a cluster that has the Cisco CallManager service and immediate divert configured.

For information about text displays, see the “Immediate Divert Phone Display Messages” section on page 27-5.

Use Legacy Immediate Divert Clusterwide Service Parameter

Immediate divert allows diversion of an incoming call to either the voice mailbox of the original called party or to the voice mailbox of the user that invokes the iDivert feature only if the Use Legacy Immediate Divert clusterwide service parameter is set to False. If the Use Legacy Immediate Divert service parameter is set to True, the user that invokes the iDivert feature can divert an incoming call only to his own voice mailbox.

Setting the Use Legacy Immediate Divert clusterwide service parameter to False allows access to voice-messaging systems that are reached over QSIG.

Allow QSIG During iDivert Clusterwide Service Parameter

Immediate divert diverts calls to voice-messaging systems that can be reached over QSIG, SIP, and QSIG-enabled H.323 devices if the Allow QSIG During iDivert clusterwide service parameter is set to True.

Immediate Divert User Response Timer Service Parameter

The value of the Immediate Divert User Response Timer service parameter determines the time that the invoker of the iDivert softkey is given to choose the party to whom to divert a call. If the invoker does not choose a party, the call remains connected.

Related Topics

- Configuration Checklist for Immediate Divert, page 27-1
- Introducing Immediate Divert, page 27-2
- System Requirements for Immediate Divert, page 27-3
- Immediate Divert Scenarios With Use Legacy Immediate Divert Service Parameter Set to False, page 27-7
- Installing and Activating Immediate Divert, page 27-10
- Configuring Immediate Divert, page 27-10
- Setting the Service Parameters for Immediate Divert, page 27-10
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Voice-Mail Pilot Configuration, Cisco Unified Communications Manager Administration Guide
- Voice-Mail Profile Configuration, Cisco Unified Communications Manager Administration Guide
• Voice Mail Connectivity to Cisco Unified Communications Manager, *Cisco Unified Communications Manager System Guide*

**Additional Cisco Documentation**

• Cisco Unified IP Phone administration documentation for Cisco Unified Communications Manager

• Cisco Unified IP Phone user documentation
Intercom

Intercom, a type of phone line, combines the functionality of a traditional line and a speed dial. With an intercom line, a user can call the intercom line of another user, which auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

The following sections provide information on intercom:

- Configuration Checklist for Intercom, page 28-1
- Introducing Intercom, page 28-2
- System Requirements, page 28-4
- Call and Line States, page 28-4
- Interactions and Restrictions, page 28-5
- Installing and Activating Intercom, page 28-7
- Configuring Intercom, page 28-8
- How to Use Intercom, page 28-38
- Related Topics, page 28-52

Configuration Checklist for Intercom

Intercom, a type of phone line, combines the functionality of a traditional line and a speed dial. With an intercom line, a user can call the intercom line of another user, which auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Users can use an intercom line to dial any other intercom line in the intercom partition, or you can preconfigure the line to target an intercom line outside the intercom partition.

Note

Users can use an intercom line only to dial other intercom lines.

Intercom allows a user to place a call to a predefined target. The called destination auto-answers the call in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless of whether the called party is busy or idle.
To ensure that the voice of the called party does not get sent back to the caller when the intercom call is automatically answered, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom means that only one-way audio exists from the caller to the called party. The called party must manually press a key to talk to the caller.

**Note**
An auto-answer tone indicates the beginning of the whisper state for both the sender and the recipient.

Table 28-1 shows the logical steps for configuring the Cisco Unified Communications Manager Intercom feature in Cisco Unified Communications Manager. For more information on intercom, see the “Introducing Intercom” section on page 28-2 and the “Related Topics” section on page 28-52.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Create intercom partition.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> When you create an intercom partition, the administration user interface will automatically generate a corresponding intercom calling search space with the same name and includes this new intercom partition initially.</td>
<td>Intercom Partition Configuration, page 28-8.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Create intercom calling search space.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Do this if you need to create an intercom calling search space other than the one that is generated automatically when you create the intercom partition.</td>
<td>Intercom Calling Search Space Configuration, page 28-15.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Create intercom translation pattern (optional).</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Create intercom directory number.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>Assign intercom directory number to a phone.</td>
<td>Directory Number Configuration, Cisco Unified Communications Manager Administration Guide Intercom Line and Speed Dial Configuration, page 28-37</td>
</tr>
</tbody>
</table>

**Introducing Intercom**

Intercom, a type of phone line, combines the functionality of a traditional line and a speed dial. With an intercom line, a user can call the intercom line of another user, which auto-answers to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

Users can use an intercom line to dial any other intercom line in the intercom partition, or you can preconfigure the line to target an intercom line outside the intercom partition.

**Note**
Users can use an intercom line only to dial other intercom lines.
**Introducing Intercom**

Intercom allows a user to place a call to a predefined target. The called destination auto-answers the call in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless of whether the called party is busy or idle.

To ensure that the voice of the called party does not get sent back to the caller when the intercom call is automatically answered, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom means that only one-way audio exists from the caller to the called party. The called party must manually press a key to talk to the caller.

---

**Note**

An auto-answer tone indicates the beginning of the whisper state for both the sender and the recipient.

---

**Intercom Directory Numbers and Default Devices**

Each intercom line needs a default device. The intercom feature requires configuration of the Default Activated Device field in the Intercom Directory Number Configuration window to make an intercom line display as active. The intercom line displays only on the designated default device.

When the administrator assigns an intercom line to a device, the system sets the device as the default device for the intercom line if not set previously. The administrator can modify the default device for the intercom line. When the administrator changes the default device to a different device, the intercom line gets removed from the original device, even though the intercom line may still be assigned to the original device.

You can assign an intercom line to a device profile. Only when a user uses a device profile to log in to the default device that matches the default device of the intercom line does the intercom line become available. Otherwise, no intercom line displays when the user logs in.

See the “Intercom Directory Number Configuration” section on page 28-28 for configuration details.

---

**Note**

If an intercom line has been configured and assigned to a phone but fails to display on the phone, check that the Default Activated Device value is set to this device for this intercom line. If that configuration has taken place, check that the phone has been reset.

---

**Intercom Directory Numbers and Cisco Extension Mobility**

Be aware that intercom directory numbers (lines) are restricted to one device per intercom line. Because Cisco Extension Mobility is widely used, mobile users need the intercom feature but need it to be available only on a single device. You can assign intercom lines to either a regular device or to an extension mobility profile, but the system needs to enforce that an intercom line gets associated to either a regular device or to an extension mobility profile.

Because an extension mobility profile can be used on more than one phone simultaneously, use the Default Activated Device field to specify which device can display this intercom line. Intercom lines that are not used for extension mobility also require configuration of the Default Activated Device field.

The “Intercom” section of the “Cisco Extension Mobility” chapter provides additional details about upgrading from Release 6.0(1) of Cisco Unified Communications Manager to Release 6.1(1) or later.
System Requirements

The system requirements for the intercom feature follow:

- Cisco Unified Communications Manager Release 6.0 or later
- Microsoft Internet Explorer (IE) 7 or Internet Explorer 8 or FireFox 3.x or Safari 4.x
- Cisco Unified IP Phones firmware release 8.3(1) or later

Intercom Support for Cisco Unified IP Phones

The list of devices that support the Intercom feature varies per version and device pack. Use the Cisco Unified Reporting application to generate a complete list of devices that support the Intercom feature for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
     - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
     - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
     - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click System Reports in the navigation bar.

3. In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.

4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

5. To generate a report of all devices that support Intercom, choose these settings from the respective drop-down list boxes and click the Submit button:
   - Product: All
   - Feature: Intercom

   The List Features pane displays a list of all devices that support the Intercom feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Call and Line States

Intercom introduces a new call state for the intercom line, Whisper. Intercom also uses the existing Idle, Connected, Offhook, and Digits After First line states.

Because only one intercom call can occur at a time, the intercom call state maps directly to the line state, and call sort rules will remain unaffected.
Table 28-2 lists the intercom call and line states.

### Table 28-2  Intercom Call and Lines States

<table>
<thead>
<tr>
<th>Description</th>
<th>Idle</th>
<th>Whisper</th>
<th>Off hook</th>
<th>Digits After First</th>
<th>Connected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Idle intercom state</td>
<td>During whisper, the recipient receives the initiator voice, but the initiator does not receive the recipient voice. Callers on any other active calls with the recipient do not receive the initiator voice.</td>
<td>Only present when a target has not been preconfigured and an intercom target must be dialed.</td>
<td>Only present when a target has not been preconfigured and an intercom target must be dialed.</td>
<td>Connected specifies the connected state for the Intercom feature.</td>
</tr>
<tr>
<td>LED Behavior</td>
<td>LED not illuminated</td>
<td>Feature Key: Solid Amber</td>
<td>Feature Key: Solid Amber</td>
<td>Feature Key: Solid Amber</td>
<td>Feature Key: Solid Green</td>
</tr>
<tr>
<td>Icon</td>
<td>Idle</td>
<td>Whisper</td>
<td>Whisper</td>
<td>Whisper</td>
<td>Connected</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>Default Cisco Unified Communications Manager Template</td>
<td>Connected No Feature</td>
<td>Intercom Off hook</td>
<td>Default Unified CM Digits After First template, Connected No Feature.</td>
<td>Connected No Feature</td>
</tr>
<tr>
<td>Other</td>
<td>An auto-answer tone precedes whisper.</td>
<td>“Inside” dial tone</td>
<td></td>
<td>No dial tone</td>
<td></td>
</tr>
</tbody>
</table>

### Interactions and Restrictions

The following sections describe the interactions and restrictions that are associated with intercom:

- Interactions, page 28-5
- Restrictions, page 28-7

### Interactions

The following sections describe how intercom interacts with Cisco Unified Communications Manager applications and call processing:

- Bulk Administration Tool, page 28-6
- Barge, page 28-6
- Do Not Disturb (DND), page 28-6
- Call Preservation, page 28-6
- Cisco Unified Survivable Remote Site Telephony (SRST), page 28-6
- Cisco Unified Communications Manager Assistant, page 28-6
- CTI, page 28-6
Bulk Administration Tool

The Cisco Unified Communications Manager administrator can use the Bulk Administration Tool (BAT) to add many intercom users at once instead of adding users individually. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

Barge

When the intercom destination is a barge target, the Cisco Unified IP Phone can still support whisper intercom.

When the destination caller opts to talk to the intercom caller by pressing the intercom button, the original call has been put on hold, and the barge initiator will get released.

Do Not Disturb (DND)

The intercom call will override DND on the destination phone.

Call Preservation

When a call is preserved, the end user needs to hang up before the phone can reregister with Cisco Unified Communications Manager. When the intercom call is in whisper mode, it represents a one-way medium, and the terminating side might have no user at all; therefore, only the intercom call in talkback mode will get preserved. (Whisper intercom will not get preserved.)

Cisco Unified Survivable Remote Site Telephony (SRST)

When Cisco Unified IP Phones register with SRST, the phones do not register intercom lines; therefore, the intercom feature will not be available when the phones are registered with SRST.

Cisco Unified Communications Manager Assistant

See the Cisco Unified Communications Manager Assistant Configuration Wizard chapter in the Cisco Unified Communications Manager Administration Guide.

CTI

You can use CTI/JTAPI/TSP to set or modify the preconfigured target directory number for an intercom line. You will receive notification if the target directory number is updated or reconfigured through Cisco Unified Communications Manager Administration.

Be aware that CTI/JTAPI/TSP is backward compatible if the intercom line is not configured to be controlled by the application. If the intercom line is configured in the application user list, you may have to make changes and test the compatibility.
Cisco Extension Mobility

The intercom feature interacts with Cisco Extension Mobility. The system presents an intercom line to a user who uses Cisco Extension Mobility to log in to a phone that supports the intercom feature if the device profile that the user uses to log in has an intercom line that is provisioned. The phone must be the default device for that intercom line.

See the “Intercom Directory Number Configuration” section on page 28-28 and to the “Cisco Extension Mobility” section on page 9-1 for configuration details.

Internet Protocol Version 6 (IPv6)

Intercom can support phones with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. During an intercom call, the talkback mode establishes media streams with the same IP version as the media stream that is used when the caller initiates intercom. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

Restrictions

The following restrictions apply to the Intercom feature:

- Intercom calls do not follow a coverage path.
- Hold—The system does not allow intercom calls to be placed on hold.
- Call Forwarding—Intercom calls cannot be forwarded.
- Transfer—The system does not allow an intercom call to be transferred.
- iDivert—The system does not allow an intercom call to be diverted.
- Call Pickup/Directed Call Pickup—The call pickup groups do not include intercom calls.
- DND—Intercom overrides Do Not Disturb (DND).
- If sufficient bandwidth does not exist, the intercom call fails.
- If two intercom calls are directed to a target, the first one goes through; the second fails with a busy tone.
- Barge and cBarge—Intercom does not work with Barge and cBarge.
- Conferencing—The system does not allow intercom calls to be conferenced.
- When an active call is being monitored or recorded, the user cannot receive nor place intercom calls
- Video is not supported with intercom.

Installing and Activating Intercom

Because intercom comes standard with Cisco Unified Communications Manager Release 6.0 and later, it automatically gets installed and activated.
Configuring Intercom

To use the intercom feature, both the caller and called phones require a dedicated intercom line button. This line will have its own Directory Number (DN), which is its intercom code, and partition (intercom group). The Calling Search Space for this intercom line gets used to restrict the access of intercom destination from this phone.

**Note**  
To guarantee that no accidental use of the intercom feature occurs by an unauthorized phone, users cannot access intercom partition and intercom calling search space from other administrative windows, except under the intercom feature.

**Note**  
The system does not allow an intercom line to be shared on multiple devices. It should not have any other feature-related configuration, such as forward, pickup, voice mail profile, and so on.

**Tip**  
A phone can have more than one intercom button that is assigned.

This section contains information on the following topics:

- Intercom Partition Configuration, page 28-8
- Intercom Calling Search Space Configuration, page 28-15
- Intercom Translation Pattern Configuration, page 28-20
- Intercom Directory Number Configuration, page 28-28

**Tip**  
Before you configure intercom, review the “Configuration Checklist for Intercom” section on page 28-1.

Intercom Partition Configuration

An intercom partition contains a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. For more information about partitions, see “Partitions and Calling Search Spaces” in the *Cisco Unified Communications Manager System Guide*.

Use the following topics to find, add, update, or delete intercom partitions:

- Adding an Intercom Partition, page 28-9
- Finding an Intercom Partition, page 28-9
- Configuring an Intercom Partition, page 28-10
- Intercom Partition Configuration Settings, page 28-11
- Synchronizing an Intercom Partition With Affected Devices, page 28-13
- Deleting an Intercom Partition, page 28-14
- Intercom Calling Search Space Configuration, page 28-15
Adding an Intercom Partition

You can add a new intercom partition by using the following procedure.

Procedure

Step 1  From the Cisco Unified Communications Manager Administration window, click **Call Routing > Intercom > Intercom Route Partition**.

The Find and List Intercom Partitions window displays.

Step 2  Click the **Add New** button.

An Add New Intercom Partition window displays.

Step 3  Under the Intercom Partition Information section, in the Name box, enter the name and description of the intercom partition that you want to add.

**Note** To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (",") to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description.

The Find and List Intercom Partitions window displays.

Step 4  Continue with Step 2 of the “Finding an Intercom Partition” section on page 28-9

Finding an Intercom Partition

The Find and List window for intercom partitions allows you to search for an intercom partition, which is a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

Because you might have several intercom partitions in your network, Cisco Unified Communications Manager lets you locate specific intercom partitions based on specific criteria. Use the following procedure to locate intercom partitions.

**Note** During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom partition search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom partition search preferences until you modify your search.

Procedure

Step 1  Choose **Call Routing > Intercom > Intercom Route Partition**.

The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.
Configuring Intercom

Step 2  To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

Note  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Intercom Calling Search Space Configuration” section on page 28-15.

Configuring an Intercom Partition

Perform the following procedure to configure an intercom partition.

Note  When you add a new intercom partition, Cisco Unified Communications Manager automatically adds a new intercom calling search space that contains only the new partition. You can modify the new intercom calling search space later.

Note  Be aware that intercom partition and intercom calling search space cannot be mixed with partition and calling search space for regular lines.
Chapter 28      Intercom

Configuring Intercom

Procedure

Step 1  In the menu bar, choose Call Routing > Intercom > Intercom Route Partition.
The Find and List Intercom Partitions window displays.
Locate the partition that you want to configure by using the steps described in “Finding an Intercom Partition” section on page 28-9, and continue with Step 2.

Step 2  Enter the appropriate settings that are described in Table 28-3.

Step 3  Click Save.
The Intercom Partition Configuration window displays

Step 4  Enter the appropriate settings that are described in Table 28-5.
If you are updating an intercom partition, click Reset or use the Apply Config button described in the “Synchronizing an Intercom Partition With Affected Devices” section on page 28-13.

Additional Information
See the “Intercom Calling Search Space Configuration” section on page 28-15.

Intercom Partition Configuration Settings

An intercom partition contains a list of route patterns [directory number (DN) and route patterns]. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. For more information about partitions, see “Partitions and Calling Search Spaces” in the Cisco Unified Communications Manager System Guide.
Table 28-3 describes the intercom partition configuration settings for adding new intercom partitions. For related procedures, see the “Intercom Calling Search Space Configuration” section on page 28-15.

### Table 28-3  Add New Intercom Partition(s) Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Intercom Partition Information Name, Description | Enter a name in the name box. Ensure each intercom partition name is unique to the route plan. Intercom partition names can contain a-z, A-Z and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_).  
**Note** The length of the intercom partition names limits the maximum number of intercom partitions that can be added to an intercom calling search space. Table 28-4 provides examples of the maximum number of intercom partitions that can be added to an intercom calling search space if intercom partition names are of fixed length. 
Follow the intercom partition name by a comma (,); then, enter a description on the same line as the Partition Name. The description can include up to 50 characters in any language, but it cannot include double-quotes (“”), angle brackets (<>), square bracket ([ ]), ampersand (&), and percentage sign (%). 
If you do not enter a description, Cisco Unified Communications Manager automatically enters the intercom partition name in this field. 
Use a new line for each intercom partition and description.  

Timesaver  
Use concise and descriptive names for your intercom partitions. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify an intercom partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.

Tip  
You can enter multiple intercom partitions at the same time by entering the intercom partition name and description, if applicable, in the Intercom Partition Information Name text box. Remember to use one line for each intercom partition entry and to separate the intercom partition name and description with a comma.  

Table 28-4 provides examples of the maximum number of intercom partitions that can be added to an intercom calling search space if partition names are of fixed length. See “Partition Name Limitations” in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.
## Configuring Intercom

Table 28-5 provides descriptions of the information needed to configure an existing intercom partition.

### Table 28-5 Intercom Partition Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intercom Partition Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the intercom partition that you selected displays in this box.</td>
</tr>
<tr>
<td>Description</td>
<td>If you entered a description of the intercom partition that you selected, it displays here. If you did not enter a description when you added the intercom partition, you can add it now.</td>
</tr>
<tr>
<td>Time Schedule</td>
<td>The drop-down list is populated with time schedules that you can add from Call Routing &gt; Class of Control &gt; Time Schedule. See “Time Schedule Configuration” in the Cisco Unified Communications Manager Administration Guide for details about how to configure time schedules.</td>
</tr>
</tbody>
</table>
| Time Zone              | • If you want the time zone to be the same as the originating device, click the radio button next to Originating Device.  
                          • If you want to set a specific time zone, click the Specific Time Zone radio button and select the correct time zone from the drop-down list. |

**Additional Information**

See the “Intercom Calling Search Space Configuration” section on page 28-15.

### Synchronizing an Intercom Partition With Affected Devices

To synchronize devices with an intercom partition that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

**Procedure**

1. **Step 1** Choose Call Routing > Intercom > Intercom Route Partition.
   The Find and List Intercom Partitions window displays.
2. **Step 2** Choose the search criteria to use.
3. **Step 3** Click Find.
   The window displays a list of intercom partitions that match the search criteria.
Step 4  Click the intercom partition to which you want to synchronize applicable devices. The Intercom Partition Configuration window displays.

Step 5  Make any additional configuration changes.

Step 6  Click Save.

Step 7  Click Apply Config.

The Apply Configuration Information dialog displays.

Note  If devices that are associated with the intercom partition get reset, calls on affected gateways may drop.

Step 8  Click OK.

Additional Information

See the “Intercom Calling Search Space Configuration” section on page 28-15.

Deleting an Intercom Partition

The following procedure describes how to delete an intercom partition.

Before You Begin

You cannot delete an intercom partition if it is assigned to an item such as calling search space or to a route pattern. To find out which calling search spaces or other items are using the intercom partition, choose Dependency Records from the Related Links drop-down list box in the Intercom Partition Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2 of the Cisco Unified Communications Manager Administration Guide. If you try to delete a partition that is in use, Cisco Unified Communications Manager displays a message. Before deleting a partition that is currently in use, you must perform either or both of the following tasks:

- Assign a different intercom partition to any intercom calling search spaces, devices, or other items that are using the intercom partition that you want to delete.
- Delete the intercom calling search spaces, devices, or other items that are using the intercom partition that you want to delete.

Procedure

Step 1  In the menu bar, choose Call Routing > Intercom > Intercom Route Partition.

Step 2  Locate the intercom partition that you want to delete. See the “Finding an Intercom Partition” section on page 28-9.

Step 3  Check the check box of the intercom partition that you want to delete and click Delete Selected.

Tip  You can delete all the intercom partitions in the list by clicking Select All and then clicking Delete Selected.
A message displays that states that you cannot undo this action.

**Step 4**

To delete the intercom partition, click **OK** or to cancel the deletion, click **Cancel**.

**Caution**

Before initiating this action, check carefully to ensure that you are deleting the correct intercom partition. You cannot retrieve deleted intercom partitions. If an intercom partition is accidentally deleted, you must rebuild it.

**Tip**

You can also delete an intercom partition by locating and displaying the partition that you want to delete and clicking **Delete**.

**Additional Information**

See the “Intercom Calling Search Space Configuration” section on page 28-15.

## Intercom Calling Search Space Configuration

An intercom calling search space comprises an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

For more detailed information on calling search spaces and partitions, see “Partitions and Calling Search Spaces” in the *Cisco Unified Communications Manager System Guide*.

Use the following topics to find, add, update, copy, or delete a calling search space:

- Finding an Intercom Calling Search Space, page 28-15
- Configuring an Intercom Calling Search Space, page 28-16
- Intercom Calling Search Space Configuration Settings, page 28-17
- Deleting an Intercom Calling Search Space, page 28-19

### Finding an Intercom Calling Search Space

The Find and List window for intercom calling search spaces allows you to search for an intercom calling search space, which is an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the intercom partitions that calling devices search when they are attempting to complete a call.

Because you might have several intercom calling search spaces in your network, Cisco Unified Communications Manager lets you locate specific intercom calling search spaces by using specific criteria as the basis. Use the following procedure to locate intercom calling search spaces.

**Note**

During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom calling search space search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom calling search space search preferences until you modify your search.
Configuring Intercom

Procedure

**Step 1**  Choose Call Routing > Intercom > Intercom Calling Search Space.

The Find and List Intercom Calling Search Spaces window displays. Records from an active (prior) query may also display in the window.

**Step 2**  To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

**Note**  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

**Step 3**  Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Note**  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

**Step 4**  From the list of records that display, click the link for the record that you want to view.

**Note**  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

**Additional Topics**
See the “Intercom Translation Pattern Configuration” section on page 28-20.

Configuring an Intercom Calling Search Space

The following procedure describes how to copy, add and update an intercom calling search space.

Procedure

**Step 1**  In the menu bar, choose Call Routing > Intercom > Intercom Calling Search Space.
Step 2  Perform one of the followings tasks:

- To copy an existing intercom calling search space, locate the appropriate intercom calling search space as described in “Finding an Intercom Calling Search Space” section on page 28-15. Click the Copy button next to the intercom calling search space that you want to copy. The window displays the copy of the intercom calling search space. Change the Intercom Calling Search Space Name, and continue with Step 3.

- To add an intercom calling search space, click the Add New button, and continue with Step 3.

Note  To add more intercom calling search spaces, click Add New and repeat this procedure.

- To update an existing intercom calling search space, locate the appropriate intercom calling search space as described in “Finding an Intercom Calling Search Space” section on page 28-15, and continue with Step 3.

Step 3  Enter the appropriate settings as described in Table 28-6.

Step 4  Click Save.

Additional Topics  See the “Intercom Translation Pattern Configuration” section on page 28-20.

Intercom Calling Search Space Configuration Settings

An intercom calling search space comprises an ordered list of intercom route partitions that are typically assigned to devices. Intercom calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.

For more detailed information on calling search spaces and partitions, see “Partitions and Calling Search Spaces” in the Cisco Unified Communications Manager System Guide.

Table 28-6 describes the intercom calling search space configuration settings. For a list of related procedures, see the “Related Topics” section on page 28-52.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name in the Intercom Calling Search Space Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each calling search space name is unique to the system.</td>
</tr>
</tbody>
</table>

Note  Use concise and descriptive names for your intercom calling search spaces. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a calling search space. For example, CiscoDallasMetroCS identifies a calling search space for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.
Table 28-6  Intercom Calling Search Space Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description in the Description field. The description can include up to 50 characters in any language, and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_), but it cannot include double-quotes (“”), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
</tbody>
</table>

Intercom Route Partitions for this Calling Search Space

<table>
<thead>
<tr>
<th>Available Intercom Partitions</th>
<th>Choose an intercom partition in the Available Intercom Partitions list box and add it to the Selected Intercom Partitions list box by clicking the arrow button between the two list boxes. To add a range of intercom partitions at once, click the first intercom partition in the range; then, hold down the Shift key while clicking the last intercom partition in the range. Click the arrow button between the two list boxes to add the range of partitions. To add multiple intercom partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple intercom partitions. Click the arrow button between the two list boxes to add the chosen intercom partitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Intercom Partitions (Ordered by highest priority)</td>
<td>To change the priority of an intercom partition, choose an intercom partition name in the Selected Intercom Partitions list box. Move the intercom partition up or down in the list by clicking the arrows on the right side of the list box.</td>
</tr>
</tbody>
</table>

Table 28-4 provides examples of the maximum number of intercom partitions that can be added to a calling search space if intercom partition names are of fixed length. See “Partition Name Limitations” in the Cisco Unified Communications Manager System Guide for details about how this maximum number is calculated.

Table 28-7  Calling Search Space Partition Limitations

<table>
<thead>
<tr>
<th>Partition Name Length</th>
<th>Maximum Number of Partitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 characters</td>
<td>170</td>
</tr>
<tr>
<td>3 characters</td>
<td>128</td>
</tr>
<tr>
<td>4 characters</td>
<td>102</td>
</tr>
<tr>
<td>5 characters</td>
<td>86</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10 characters</td>
<td>46</td>
</tr>
<tr>
<td>15 characters</td>
<td>32</td>
</tr>
</tbody>
</table>
Deleting an Intercom Calling Search Space

The following procedure describes how to delete an intercom calling search space.

**Before You Begin**

You cannot delete intercom calling search spaces that devices, lines (DNs), translation patterns, or other items are using. To find out which devices, lines, translation patterns, or other items are using the intercom calling search space, choose the **Dependency Records** from the Related Links drop-down list box in the Intercom Calling Search Space Configuration window and click **Go**. If the dependency records are not enabled for the system, the dependency records summary window displays a message. For more information about dependency records, see the “Accessing Dependency Records” section on page A-2 of the *Cisco Unified Communications Manager Administration Guide*. If you try to delete an intercom calling search space that is in use, Cisco Unified Communications Manager displays a message. Before deleting an intercom calling search space that is currently in use, you must perform either or both of the following tasks:

- Assign a different intercom calling search space to any devices, lines, or translation patterns that are using the intercom calling search space that you want to delete. See the “Intercom Directory Number Configuration” section on page 28-28 and the “Intercom Translation Pattern Configuration” section on page 28-20.

- Delete the devices, lines, or translation patterns that are using the intercom calling search space that you want to delete. See the “Removing a Directory Number from a Phone” section on page 43-26, and the “Deleting an Intercom Translation Pattern” section on page 28-28.

**Procedure**

**Step 1** In the menu bar, choose **Call Routing > Intercom > Intercom Calling Search Space**.

**Step 2** Locate the intercom calling search space that you want to delete. See the “Finding an Intercom Calling Search Space” section on page 28-15.

**Step 3** Check the check box of the intercom calling search space that you want to delete and click **Delete Selected**.

A message displays that states that you cannot undo this action.

**Step 4** To delete the intercom calling search space, Click **OK** or click **Cancel**.

**Caution**

Before initiating this action, check carefully to ensure that you are deleting the correct intercom calling search space. You cannot retrieve deleted intercom calling search spaces. If an intercom calling search space is accidentally deleted, you must rebuild it.

**Tip**

You can also delete an intercom calling search space by locating and displaying the intercom calling search space that you want to delete and clicking **Delete**.
Additional Topics
See the “Intercom Translation Pattern Configuration” section on page 28-20.

Intercom Translation Pattern Configuration

Cisco Unified Communications Manager uses intercom translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number.

Use the following topics to add, update, copy, or delete an intercom translation pattern:

- Finding an Intercom Translation Pattern, page 28-20
- Configuring an Intercom Translation Pattern, page 28-21
- Intercom Translation Pattern Configuration Settings, page 28-22
- Deleting an Intercom Translation Pattern, page 28-28
- Intercom Directory Number Configuration, page 28-28

Finding an Intercom Translation Pattern

The Find and List window for intercom translation patterns allows you to search on intercom translation patterns, which Cisco Unified Communications Manager uses to manipulate dialed digits before it routes a call.

Because you might have several intercom translation patterns in your network, Cisco Unified Communications Manager lets you locate specific intercom translation patterns by using specific criteria as the basis. Use the following procedure to locate intercom translation patterns.

**Note**
During your work in a browser session, Cisco Unified Communications Manager Administration retains your intercom translation pattern search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your intercom translation pattern search preferences until you modify your search or close the browser.

**Procedure**

**Step 1** Choose Call Routing > Intercom > Intercom Translation Pattern.

The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.
Step 3  Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.

Note  To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Intercom Directory Number Configuration” section on page 28-28.

Configuring an Intercom Translation Pattern

This section describes how to configure an intercom translation pattern.

Before You Begin
Configure the following Cisco Unified Communications Manager intercom items before configuring an intercom translation pattern:
- Intercom partition
- Intercom route filter
- Intercom calling search space

Procedure

Step 1  Choose Call Routing > Intercom > Intercom Translation Pattern.

The Find and List Intercom Translation Patterns window displays.

Step 2  Perform one of the followings tasks:
- To copy an existing intercom translation pattern, locate the appropriate intercom translation pattern as described in the “Finding an Intercom Translation Pattern” section on page 28-20, click the Copy button next to the intercom translation pattern that you want to copy, and continue with Step 3.
- To add a new intercom translation pattern, click the Add New button, and continue with Step 3.
Step 3 In the Intercom Translation Pattern Configuration window that displays, enter the appropriate configuration settings as described in Table 28-6.

Step 4 Click Save.

| Note | Ensure that the intercom translation pattern, that uses the selected partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows if you receive an error that indicates duplicate entries. |

The Intercom Translation Pattern Configuration window displays the newly configured intercom translation pattern.

Additional Information
See the “Intercom Directory Number Configuration” section on page 28-28.

Intercom Translation Pattern Configuration Settings
Cisco Unified Communications Manager uses intercom translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number.

Table 28-8 describes the available fields in the Intercom Translation Pattern Configuration window. For related procedures, see the “Related Topics” section on page 28-52.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Definition</td>
<td></td>
</tr>
<tr>
<td>Intercom Translation Pattern</td>
<td>Enter the intercom translation pattern, including numbers and wildcards (do not use spaces), in the Intercom Translation Pattern field. For example, for the NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and ^+, which represents the international escape character +. If you leave this field blank, you must select a partition from the Partition drop-down list box.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that the intercom translation pattern, which uses the chosen intercom partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number if you receive a message that indicates duplicate entries. Alternatively, check the route plan report if you receive a message that indicates duplicate entries.</td>
</tr>
</tbody>
</table>
Configuring Intercom

Partition

Choose an intercom partition. If you do not want to assign an intercom partition, choose <None>. If you choose <None>, you must enter a value in the Intercom Translation Pattern field.

You can configure the number of intercom partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom partitions exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Partitions window. Find and choose an intercom partition name (see the “Finding an Intercom Partition” section on page 28-9).

Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Note: Make sure that the combination of intercom translation pattern, route filter, and intercom partition is unique within the Cisco Unified Communications Manager cluster.

Description

Enter a description for the intercom translation pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes (“”), percentage sign (%), ampersand (&), or angle brackets (<>).

Numbering Plan

Choose a numbering plan.

If your intercom translation pattern includes the @ wildcard, you may choose a numbering plan. The optional act of choosing a numbering plan restricts certain number patterns.

Route Filter

Choosing an optional route filter restricts certain number patterns. See the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the Cisco Unified Communications Manager System Guide and the “Route Filter Configuration Settings” section on page 30-1 section in the Cisco Unified Communications Manager Administration Guide for more information.

The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.

If more than 250 route filters exist, the Find button displays next to the drop-down list box. Click the Find button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click Add Selected.

Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
<td>Choose an intercom partition. If you do not want to assign an intercom partition, choose &lt;None&gt;. If you choose &lt;None&gt;, you must enter a value in the Intercom Translation Pattern field. You can configure the number of intercom partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom partitions exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Partitions window. Find and choose an intercom partition name (see the “Finding an Intercom Partition” section on page 28-9). Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters. Note: Make sure that the combination of intercom translation pattern, route filter, and intercom partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the intercom translation pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes (“”), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Numbering Plan</td>
<td>Choose a numbering plan. If your intercom translation pattern includes the @ wildcard, you may choose a numbering plan. The optional act of choosing a numbering plan restricts certain number patterns.</td>
</tr>
<tr>
<td>Route Filter</td>
<td>Choosing an optional route filter restricts certain number patterns. See the “Wildcards and Special Characters in Route Patterns and Hunt Pilots” section in the Cisco Unified Communications Manager System Guide and the “Route Filter Configuration Settings” section on page 30-1 section in the Cisco Unified Communications Manager Administration Guide for more information. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. If more than 250 route filters exist, the Find button displays next to the drop-down list box. Click the Find button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click Add Selected. Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
</tbody>
</table>
### Table 28-8 Translation Pattern Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence</td>
<td>Choose an MLPP precedence setting for this intercom translation pattern from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td>- Executive Override—Highest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Flash Override—Second highest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Flash—Third highest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Immediate—Fourth highest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Priority—Fifth highest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Routine—Lowest precedence setting for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td>- Default—Does not override the incoming precedence level but rather lets it pass unchanged.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>See the “Precedence” section in the “Multilevel Precedence and Preemption” chapter for more information.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the intercom calling search space for which you are adding an intercom translation pattern, if necessary.</td>
</tr>
<tr>
<td></td>
<td>You can configure the number of intercom calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom calling search spaces exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Calling Search Space window. Find and choose an intercom calling search space name (see the “Finding an Intercom Calling Search Space” section on page 28-15).</td>
</tr>
<tr>
<td>Route Option</td>
<td>The Route Option designation indicates whether you want this intercom translation pattern to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button.</td>
</tr>
<tr>
<td></td>
<td>If you choose the Block this pattern radio button, you must choose the reason for which you want this intercom translation pattern to block calls. Choose a value from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td>- No Error</td>
</tr>
<tr>
<td></td>
<td>- Unallocated Number</td>
</tr>
<tr>
<td></td>
<td>- Call Rejected</td>
</tr>
<tr>
<td></td>
<td>- Number Changed</td>
</tr>
<tr>
<td></td>
<td>- Invalid Number Format</td>
</tr>
<tr>
<td></td>
<td>- Precedence Level Exceeded</td>
</tr>
<tr>
<td>Provide Outside Dial Tone</td>
<td>Outside dial tone indicates that Cisco Unified Communications Manager routes the calls off the local network. Check this check box for each intercom translation pattern that you consider to be off network.</td>
</tr>
</tbody>
</table>
### Table 28-8 Translation Pattern Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent Priority</td>
<td>If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately. By default, the Urgent Priority check box displays as checked. Unless your dial plan contains overlapping patterns or variable length patterns that contain !, Cisco recommends that you do not uncheck the check box.</td>
</tr>
</tbody>
</table>

**Calling Party Transformations**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Calling Party’s External Phone Number Mask</td>
<td>Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.</td>
</tr>
<tr>
<td>Calling Party Transform Mask</td>
<td>Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place. See the “Route List Configuration Settings” section on page 32-1 of the <em>Cisco Unified Communications Manager Administration Guide</em> for more detailed information.</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits. Valid entries for the NANP include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. <strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
</tbody>
</table>
### Calling Line ID Presentation
Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis.

Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this intercom translation pattern.

Choose **Default** if you do not want to change calling line ID presentation. Choose **Allowed** if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose **Restricted** if you want Cisco Unified Communications Manager to block the display of the calling number.

For more information about this field, see Table 16-8 in the “Calling Party Number Transformations Settings” section in the *Cisco Unified Communications Manager System Guide*.

**Note**
Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See “Device Profile Configuration Settings” and Table 67-1 in the “Configuring Speed-Dial Buttons or Abbreviated Dialing” section of the *Cisco Unified Communications Manager Administration Guide* for information about the Ignore Presentation Indicators (internal calls only) field. For more information about call display restrictions, see the Call Display Restrictions chapter of this guide.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Line ID Presentation</td>
<td>Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this intercom translation pattern. Choose <strong>Default</strong> if you do not want to change calling line ID presentation. Choose <strong>Allowed</strong> if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose <strong>Restricted</strong> if you want Cisco Unified Communications Manager to block the display of the calling number. For more information about this field, see Table 16-8 in the “Calling Party Number Transformations Settings” section in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>

---

### Calling Name Presentation
Cisco Unified Communications Manager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis.

Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party name on the called party phone display for this intercom translation pattern.

Choose **Default** if you do not want to change calling name presentation. Choose **Allowed** if you want Cisco Unified Communications Manager to display the calling name information. Choose **Restricted** if you want Cisco Unified Communications Manager to block the display of the calling name information.

For more information about this field, see Table 16-8 in the “Calling Party Number Transformations Settings” section in the *Cisco Unified Communications Manager System Guide*. |
### Table 28-8 Translation Pattern Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Party Transformations</td>
<td></td>
</tr>
<tr>
<td>Connected Line ID Presentation</td>
<td>Cisco Unified Communications Manager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party phone number on the calling party phone display for this intercom translation pattern. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party phone number. For more information about this field, see Table 16-11 in the “Connected Party Presentation and Restriction Settings” section in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Connected Name Presentation</td>
<td>Cisco Unified Communications Manager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party name on the calling party phone display for this intercom translation pattern. Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party name. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party name. For more information about this field, see Table 16-11 in the “Connected Party Presentation and Restriction Settings” section in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Called Party Transformations</td>
<td></td>
</tr>
<tr>
<td>Discard Digits</td>
<td>Choose the discard digits instructions that you want to be associated with this intercom translation pattern. See the “Discard Digits Instructions” section in the Cisco Unified Communications Manager System Guide for more information. Note The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</td>
</tr>
<tr>
<td>Called Party Transform Mask</td>
<td>Enter a transformation mask value. Valid entries for the NANP include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed.</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits. Valid entries for the NANP include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. Note The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
</tbody>
</table>
Deleting an Intercom Translation Pattern

This section describes how to delete an intercom translation pattern.

Procedure

Step 1  Choose Call Routing > Intercom > Intercom Translation Pattern.

Step 2  Locate the intercom translation pattern that you want to delete. See the “Finding an Intercom Translation Pattern” section on page 28-20.

Step 3  Check the check box of the intercom translation pattern that you want to delete and click Delete Selected.

A message displays that states that you cannot undo this action.

Step 4  To delete the intercom translation pattern, click OK or to cancel the deletion, click Cancel.

Caution

Check carefully to ensure that you are deleting the correct intercom translation pattern before you initiate this action. You cannot retrieve deleted intercom translation patterns. If you accidentally delete an intercom translation pattern, you must rebuild it.

Tip

You can also delete an intercom translation pattern by locating and displaying the intercom translation pattern that you want to delete and clicking Delete.

Intercom Directory Number Configuration

The following sections provide information about working with and configuring intercom directory numbers (DNs) in Cisco Unified Communications Manager Administration:

- Intercom Directory Number Configuration Overview, page 28-29
- Finding an Intercom Directory Number, page 28-29
- Configuring an Intercom Directory Number, page 28-30
- Intercom Directory Number Configuration, page 28-28
- Synchronizing an Intercom Directory Number With Affected Devices, page 28-37

Additional Topics

See the “Related Topics” section on page 28-52.
Intercom Directory Number Configuration Overview

Using Cisco Unified Communications Manager Administration, configure and modify intercom directory numbers (DNs) that are assigned to specific phones. These sections provide instructions for working with intercom directory numbers.

Note
Be aware that a partition is required for intercom directory numbers.

Note
Intercom directory numbers require configuration of the Default Activated Device field in the Intercom Directory Number Configuration window as specified in the “Default Activated Device” section on page 28-36 if the intercom directory number is to be active. You can also configure intercom directory numbers for use with Cisco Extension Mobility as specified in the same description.

Additional Topics
See the “Related Topics” section on page 28-52.

Finding an Intercom Directory Number

The Find and List window for intercom directory numbers allows you to search for intercom directory numbers, which are directory numbers that are used for the intercom feature and are assigned to specific phones. Use the following procedure to find an intercom directory number (DN).

Procedure

Step 1
Choose Call Routing > Intercom > Intercom Directory Number.
The Find and List Intercom Directory Numbers window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
  • From the first drop-down list box, select a search parameter.
  • From the second drop-down list box, select a search pattern.
  • Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3
Click Find.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.
**Configuring an Intercom Directory Number**

Follow these instructions to add or update an intercom directory number (DN). You can configure the call forward, call pickup, and MLPP phone features while you are adding the directory number.

**Procedure**

**Step 1** Choose **Call Routing > Intercom > Intercom Directory Number**. The Find and List Intercom Directory Numbers window displays.

**Step 2** To locate a specific intercom directory number, enter search criteria and click **Find**. A list of intercom directory numbers that match the search criteria displays.

**Step 3** Perform one of the following tasks:

- To add an intercom directory number, click the **Add New** button to add a new intercom directory number. The Intercom Directory Number Configuration window displays.
Note: The Phone Configuration window provides an alternate method for adding a directory number. Use the Device > Phone menu option and create a new phone or search for an existing phone. After you create the new phone or display the existing phone, click either the Line [1] - Add a new DN or Line [2] - Add a new DN link in the Association Information area on the left side of the Phone Configuration window. The Directory Number Configuration window displays, and you can continue with Step 4 of this procedure.

- To update an intercom directory number, click the intercom directory number that you want to update. The Intercom Directory Number Configuration window displays.

**Step 4**
Update the appropriate settings as described in Table 28-9.

**Step 5**
Click Save.

Note: See the “Synchronizing an Intercom Directory Number With Affected Devices” section on page 28-37 before deciding whether to continue to Step 6 below.

**Step 6**
Click Reset Phone. For more information, see the “Tips About Resetting a Phone” section in the Cisco Unified Communications Manager Administration Guide.

Tip: If you need more than two lines, you can increase the lines by modifying the phone button template for the phone type. Some phone types, however, only support one or two lines (such as Cisco Unified IP Phone 7906).

Note: Restart devices as soon as possible. During this process, the system may drop calls on gateways.

---

**Intercom Directory Number Configuration Settings**

For intercom, you must configure an intercom directory number.

Tip: You can assign patterns to intercom directory numbers; for example, 352XX. To avoid user confusion when you assign a pattern to an intercom directory number, add text or digits to the intercom DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for a intercom directory number only after you add the intercom directory number and you associate the intercom directory number with a phone.)

For example, add the user name to the line text label and internal caller ID, but add the outside line number to the external number mask, so, when the calling information displays, it says John Chan, not 352XX.
Note
Be aware that a partition is required for intercom directory numbers.

Note
Intercom directory numbers require configuration of the Default Activated Device field in the Intercom Directory Number Configuration window as specified in the “Default Activated Device” section on page 28-36 if the intercom directory number is to be active. You can also configure intercom directory numbers for use with Cisco Extension Mobility as specified in the same description.

Table 28-9 describes the fields that are available in the Intercom Directory Number Configuration window. For related procedures, see the “Related Topics” section on page 28-52.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intercom Directory Number Information</strong></td>
<td></td>
</tr>
<tr>
<td>Intercom Directory Number</td>
<td>Enter a dialable phone number. Values can include numeric characters and route pattern wildcards and special characters except for (.@). The intercom directory number that you enter can appear in more than one intercom partition. At the beginning of the intercom directory number, enter + if you want to use the international escape character +. For this field, + does not represent a wildcard; instead, entering + represents a dialed digit.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>Choose the intercom partition to which the intercom directory number belongs. Make sure that the intercom directory number that you enter in the Intercom Directory Number field is unique within the intercom partition that you choose. You can configure the number of intercom partitions that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom partitions exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Partition window. Enter a partial intercom partition name in the <strong>List items where Name contains</strong> field. Click the desired intercom partition name in the list of intercom partitions that displays in the <strong>Select item to use</strong> box and click Add Selected. Note To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAadmin Parameters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the intercom directory number and intercom route partition. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), or angle brackets (&lt;&gt;).</td>
</tr>
</tbody>
</table>
Chapter 28  Intercom

Configuring Intercom

Alerting Name

Enter a name that you want to display on the phone of the caller. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks:

- Forwards the name of the caller that is assigned to the directory number.
- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration.

If you do not configure an alerting name, “Name Not Available” may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field.

Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.

ASCII Alerting Name

This field provides the same information as the Alerting Name field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the Alerting Name ASCII field.

Allow Control of Device from CTI

Check this check box to allow CTI to control and monitor a line on a device with which this intercom directory number is associated.

---

Table 28-9  Intercom Directory Number Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerting Name</td>
<td>Enter a name that you want to display on the phone of the caller. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks:</td>
</tr>
<tr>
<td></td>
<td>- Forwards the name of the caller that is assigned to the directory number.</td>
</tr>
<tr>
<td></td>
<td>- Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration.</td>
</tr>
<tr>
<td></td>
<td>If you do not configure an alerting name, “Name Not Available” may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field.</td>
</tr>
<tr>
<td></td>
<td>Setting the Always Display Original Dialed Number service parameter to True impacts the alerting name functionality. If you set the service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.</td>
</tr>
<tr>
<td>ASCII Alerting Name</td>
<td>This field provides the same information as the Alerting Name field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the Alerting Name ASCII field.</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
<td>Check this check box to allow CTI to control and monitor a line on a device with which this intercom directory number is associated.</td>
</tr>
</tbody>
</table>
Configuring Intercom

Chapter 28  Intercom

Associated Devices

After you associate this intercom directory number with a device, this pane displays the device with which this intercom directory number is associated.

Note  An intercom directory number can be associated with at most one device.

To edit a device with which this intercom directory number is associated, choose a device name in the Associated Devices pane and click the Edit Device button. The Phone Configuration window or Device Profile Configuration window displays for the device that you choose. See the “Cisco Unified IP Phone Configuration” chapter or the “Device Profile Configuration” chapter of the Cisco Unified Communications Manager Administration Guide for more information about configuring phones or device profiles.

To edit a line appearance that has been defined for this intercom directory number, choose a device name in the Associated Devices pane and click the Edit Line Appearance button. The Directory Number Configuration window or Device Profile Configuration window refreshes to show the line appearance for this DN on the device that you choose.

To associate a device to this intercom directory number from the list of devices in the Dissociate Devices pane, choose a device in the Dissociate Devices pane and add it to the Associated Devices pane by clicking the up arrow between the two panes.

Dissociate Devices

If you choose to dissociate an intercom directory number from a device, this pane displays the device(s) from which you dissociate this intercom directory number.

Choose a device in the Associated Devices pane and add it to the Dissociate Devices pane by clicking the down arrow between the two panes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Devices</td>
<td>After you associate this intercom directory number with a device, this pane displays the device with which this intercom directory number is associated. Note An intercom directory number can be associated with at most one device. To edit a device with which this intercom directory number is associated, choose a device name in the Associated Devices pane and click the Edit Device button. The Phone Configuration window or Device Profile Configuration window displays for the device that you choose. See the “Cisco Unified IP Phone Configuration” chapter or the “Device Profile Configuration” chapter of the Cisco Unified Communications Manager Administration Guide for more information about configuring phones or device profiles. To edit a line appearance that has been defined for this intercom directory number, choose a device name in the Associated Devices pane and click the Edit Line Appearance button. The Directory Number Configuration window or Device Profile Configuration window refreshes to show the line appearance for this DN on the device that you choose. To associate a device to this intercom directory number from the list of devices in the Dissociate Devices pane, choose a device in the Dissociate Devices pane and add it to the Associated Devices pane by clicking the up arrow between the two panes.</td>
</tr>
</tbody>
</table>

| Dissociate Devices | If you choose to dissociate an intercom directory number from a device, this pane displays the device(s) from which you dissociate this intercom directory number. Choose a device in the Associated Devices pane and add it to the Dissociate Devices pane by clicking the down arrow between the two panes. |
Intercom Directory Number Settings

Calling Search Space

From the drop-down list box, choose the appropriate intercom calling search space. An intercom calling search space comprises a collection of intercom partitions that are searched for numbers that are called from this intercom directory number. The value that you choose applies to all devices that are using this intercom directory number. For configuration information about calling search space for directory numbers, see the “Calling Search Space” section on page 28-36.

Changes result in an update of the numbers that the Call Pickup Group field lists.

You can configure calling search space for forward all, forward busy, forward no answer, forward no coverage, and forward on CTI failure directory numbers. The value that you choose applies to all devices that are using this directory number.

You must configure either primary for forward all calling search space or secondary forward all calling search space or both for call forward all to work properly. The system uses these concatenated fields (Primary CFA CSS + Secondary CFA CSS) to validate the CFA destination and forward the call to the CFA destination.

Note If the system is using partitions and calling search spaces, Cisco recommends that you configure the other call forward calling search spaces as well. When a call is forwarded or redirected to the call forward destination, the configured call forward calling search space gets used to forward the call. If the forward calling search space is None, the forward operation may fail if the system is using partitions and calling search spaces. For example, if you configure the forward busy destination, you should also configure the forward busy calling search space. If you do not configure the forward busy calling search space and the forward busy destination is in a partition, the forward operation may fail.

When you forward calls by using the CFwdAll softkey on the phone, the automatic combination of the line CSS and device CSS does not get used. Only the configured Primary CFA CSS and Secondary CFA CSS get used. If both of these fields are None, the combination results in two null partitions, which may cause the operation to fail.

If you want to restrict users from forwarding calls on their phones, you must choose a restrictive calling search space from the Forward All Calling Search Space field.

For more information, see “Partitions and Calling Search Spaces” in the Cisco Unified Communications Manager System Guide.

Table 28-9 Intercom Directory Number Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate intercom calling search space. An intercom calling search space comprises a collection of intercom partitions that are searched for numbers that are called from this intercom directory number. The value that you choose applies to all devices that are using this intercom directory number. For configuration information about calling search space for directory numbers, see the “Calling Search Space” section on page 28-36. Changes result in an update of the numbers that the Call Pickup Group field lists. You can configure calling search space for forward all, forward busy, forward no answer, forward no coverage, and forward on CTI failure directory numbers. The value that you choose applies to all devices that are using this directory number. You must configure either primary for forward all calling search space or secondary forward all calling search space or both for call forward all to work properly. The system uses these concatenated fields (Primary CFA CSS + Secondary CFA CSS) to validate the CFA destination and forward the call to the CFA destination. Note If the system is using partitions and calling search spaces, Cisco recommends that you configure the other call forward calling search spaces as well. When a call is forwarded or redirected to the call forward destination, the configured call forward calling search space gets used to forward the call. If the forward calling search space is None, the forward operation may fail if the system is using partitions and calling search spaces. For example, if you configure the forward busy destination, you should also configure the forward busy calling search space. If you do not configure the forward busy calling search space and the forward busy destination is in a partition, the forward operation may fail. When you forward calls by using the CFwdAll softkey on the phone, the automatic combination of the line CSS and device CSS does not get used. Only the configured Primary CFA CSS and Secondary CFA CSS get used. If both of these fields are None, the combination results in two null partitions, which may cause the operation to fail. If you want to restrict users from forwarding calls on their phones, you must choose a restrictive calling search space from the Forward All Calling Search Space field. For more information, see “Partitions and Calling Search Spaces” in the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
Chapter 28      Intercom

Configuring Intercom

Calling Search Space
You can configure the number of intercom calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down

### Table 28-9 Intercom Directory Number Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence Group</td>
<td>Configure this field with the presence feature. From the drop-down list box, choose a Presence Group for this intercom directory number. The selected group specifies the devices, end users, and application users that can monitor this intercom directory number. The default value for Presence Group specifies Standard Presence group, configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. See the &quot;Presence&quot; chapter for information about configuring permissions between groups.</td>
</tr>
<tr>
<td>Auto Answer</td>
<td>Choose one of the following options to activate the auto answer feature for this intercom directory number:</td>
</tr>
<tr>
<td></td>
<td>• Auto Answer with Headset</td>
</tr>
<tr>
<td></td>
<td>• Auto Answer with Speakerphone</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Make sure that the headset or speakerphone is not disabled when you choose Auto Answer with headset or Auto Answer with speakerphone.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not configure auto answer for devices that have shared lines.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For an intercom line on a CTIPort device, autoanswer-speakerphone and autoanswer-headset means that the autoanswer is on. The speakerphone or headset options do not apply to CTIPort devices; instead, it just indicates that the line is capable of auto-answering. Applications have responsibility for terminating the media on CTIPort devices and can terminate the media on either type of output device.</td>
</tr>
<tr>
<td>Default Activated Device</td>
<td>From the drop-down list box, choose a default activated device for this intercom directory number. The selected device specifies the phone on which this intercom directory number is activated by default. The drop-down list box lists only devices that support intercom. You must specify a default activated device for this intercom directory number to be active as an intercom line. If an intercom directory number is specified in a device profile that is configured for Cisco Extension Mobility, that intercom directory number will display as an intercom line only when a user logs in to the specified default activated device by using that device profile, as long as the device supports the intercom feature.</td>
</tr>
</tbody>
</table>

---

**Calling Search Space**

You can configure the number of intercom calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more intercom calling search spaces exist than the Max List Box Items enterprise parameter specifies, the **Find** button displays next to the drop-down list box. The default value for Calling Search Space is configured with installation. Intercom calling search spaces that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box. Calling search spaces are used to allow or block calling attempts between devices or users. See the "Calling Search Space" chapter for information about configuring permissions between calling search spaces.
list box. Click the Find button to display the Find and List Calling Search Spaces window. Enter a partial intercom calling search space name in the List items where Name contains field. Click the desired intercom calling search space name in the list of intercom calling search spaces that displays in the Select item to use box and click Add Selected.

Note
To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Additional Topic
See the “Related Topics” section on page 28-52.

Synchronizing an Intercom Directory Number With Affected Devices

To synchronize devices with an intercom directory number that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

Step 1 Choose Call Routing > Intercom > Intercom Directory Number.
The Find and List Intercom Directory Numbers window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find.
The window displays a list of intercom directory numbers that match the search criteria.

Step 4 Click the intercom directory number to which you want to synchronize applicable devices. The Intercom Directory Number Configuration window displays.

Step 5 Make any additional configuration changes.

Step 6 Click Save.

Step 7 Click Apply Config.
The Apply Configuration Information dialog displays.

Step 8 Click OK.

Intercom Line and Speed Dial Configuration

To configure the intercom line, perform the following procedure:

Procedure

Step 1 If you have not already done so, create the intercom partition, as described in the “Intercom Partition Configuration” section on page 28-8.
Step 2  If you have not already done so, create the intercom directory number, as described in the “Intercom Directory Number Configuration” section on page 28-28.

Step 3  Click Device > Device Settings > Phone Button Template and add the intercom line to an existing phone button template or create a new template.

Note  Be aware that the intercom line cannot be configured as the primary line.

Step 4  Choose Device > Phone and assign an intercom directory number to the intercom line.

Step 5  Configure the intercom directory number and set up intercom speed dial, if desired.

Note  You can configure the intercom line with a predefined destination (speed dial) to allow fast access.

How to Use Intercom

The following sections explain, through written word and the use of illustrations, how to use intercom.

- Case Studies, page 28-38
- Illustrated Explanation of Intercom, page 28-39

Case Studies

The following information explains how intercom works when it is initiated to an idle phone and to a busy phone.

Intercom to an Idle Phone

When Alice intercoms Bob, Bob will receive an intercom tone first, followed by the voice of Alice. Alice, however, will not hear Bob.

If Bob has his headset on, he will use it to hear Alice; otherwise, the speaker will get used.

Intercom to a Busy Phone

Bob and Carol are speaking when Alice places an intercom call to Bob. The voice of Alice voice will get mixed with the voice of Carol voice to be played to Bob; however, Alice cannot hear Bob, while Carol will continue to hear Bob.

For most cases, Carol will only hear Bob, but not Alice; however, if Bob is using speakerphone when conversing with Carol, the voices of Alice and Bob might be mixed when they are sent to Carol.

The busy phone means that an active call exists on the phone of Bob, or it represents an outgoing call that has not connected yet.

For intercom terminating caller to end the intercom call without talking to the originator, the caller needs to press I-help button followed by intercom button to bring the softkey set for intercom into focus. User then can press ‘EndCall’ softkey to end the call.
Illustrated Explanation of Intercom

The following information shows how intercom works in several different scenarios.

- Scenario 1, page 28-39
- Scenario 2, page 28-42
- Scenario 3, page 28-44
- Scenario 4, page 28-46
- Scenario 5, page 28-48

Scenario 1

The phone that belongs to Anna, while idle, receives an intercom call from Gerald who is the preconfigured intercom target.

Figure 28-1    Idle

- Before Gerald places the intercom call to Anna, her phone is idle.
  - The line key and the intercom key appear dark.
The intercom line becomes active, and a call from Gerald appears.
- The intercom key displays solid amber.
- Both phones receive auto-answer alert tones.
- Anna hears Gerald speaking, but Gerald cannot hear Anna until she addresses the intercom call.

**Note**
Pressing the Mute key will not address the intercom call; it will only cause the status line to display “That key is not active here.”
Anna addresses the intercom call by pressing the intercom line key.

- The intercom key displays solid green.

**Note**

The call timer does not reset but continues from the whisper state.
Scenario 2

Anna, while her phone is idle, places an intercom call to Gerald’s phone, the preconfigured intercom target.

Figure 28-4 Whisper
Figure 28-5    Connected

- Gerald addresses the intercom call by pressing the intercom line key.
  - The intercom key displays solid green.

Note
The call timer does not reset.
**Scenario 3**

Anna, while on a connected or held call, receives an intercom call from Gerald, the preconfigured intercom target.

![Figure 28-6 Whisper](image)

- While Anna is speaking on the phone, the preconfigured intercom line indicator flashes amber, which indicates that Gerald is calling Anna on the intercom line.
  - The line key displays solid green.
  - The intercom key displays solid amber.

**Note**

When Auto Line Select is disabled, which represents the default, the current call retains focus.

- The phone that Anna is using plays an auto-answer alert tone, followed by the voice of Gerald.
- Anna can hear Gerald, but Gerald cannot hear Anna until she addresses the intercom call.
- The current caller, who is at 9873 and is on the line with Anna, can hear Anna but cannot hear Gerald.
Figure 28-7  Connected

- Anna addresses the intercom call by pressing the intercom line key.
  - The line key flashes green.
- The intercom call gains focus, and the previous call gets put on hold.
  - The intercom line key displays solid green.

**Note**
The call timer represents the cumulative call time from the whisper state and the current connected state.
Scenario 4

Anna, while on a whispered or connected intercom call, receives a new call on the primary line.

Figure 28-8  Connected

- Anna is talking to Gerald on an intercom line when a call displays for 9824, which is her extension. The intercom call retains focus.
  - The line key flashes amber.
  - The intercom key displays solid green.
Anna accepts the incoming call by pressing the 9824 line key.
- The line key displays solid green.
- The incoming call receives focus and gets connected.
- The system clears the intercom call.
- The intercom key displays dark.
Scenario 5

Anna, while idle, places an intercom call to Gerald. The intercom line has no preconfigured target.

- All the line keys display dark.
Anna presses the intercom line key, which invokes the dial-out state.
- The intercom key displays solid amber.
- The phone receives an “inside” dial tone.

**Note**
At this time, if Anna dials any number other than an intercom number, the phone receives a fast busy tone.
Anna begins to dial, which invokes the digits after first state.
- The intercom key displays solid amber.
After Anna dials the intercom number, the whisper state exists.

- The intercom key displays solid amber.
- The phone plays an auto-answer alert.
- Gerald can hear Anna, but Anna cannot hear Gerald until he addresses the intercom call.
Gerald addresses the intercom call by pressing the intercom line key.
- Anna can see that the intercom key displays solid green.
- The call timer does not reset but, instead, continues from the whisper state.

Related Topics
- Configuration Checklist for Intercom, page 28-1
- Introducing Intercom, page 28-2
- System Requirements, page 28-4
- Call and Line States, page 28-4
- Interactions and Restrictions, page 28-5
- Installing and Activating Intercom, page 28-7
- Configuring Intercom, page 28-8
- How to Use Intercom, page 28-38
- Intercom Translation Pattern Configuration, page 28-20.
Chapter 28      Intercom

Related Topics

- Intercom Directory Number Configuration, page 28-28
- Intercom Line and Speed Dial Configuration, page 28-37
- Internet Protocol Version 6 (IPv6), page 29-1
- Troubleshooting Guide for Cisco Unified Communications Manager
Internet Protocol Version 6 (IPv6)

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

Use this information in conjunction with the document, Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x), which provides design guidelines for deploying IPv6 in your Cisco Unified Communications network.

This chapter, which provides information on IPv6 support for Cisco Unified Communications Manager and other components in the network, contains the following topics:

- Configuration Checklist for IPv6, page 29-2
- Introducing IPv6 for Cisco Unified Communications Manager, page 29-5
  - CTI Applications, page 29-5
  - Cisco Unified Communications Manager, page 29-6
  - Cisco Unified IP Phones, page 29-8
  - DHCPv6, page 29-10
  - DNS, page 29-11
  - Gateways, page 29-12
  - Media Termination Points, page 29-12
  - SIP Trunks, page 29-13
  - TFTP Server, page 29-15
- System Requirements for IPv6, page 29-16
- Interactions and Restrictions, page 29-16
- Installing and Activating IPv6, page 29-21
- Configuring IPv6, page 29-21
  - Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 29-21
  - Configuring Service and Enterprise Parameters for IPv6, page 29-25
  - Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration, page 29-27
Providing Information to End Users, page 29-32
Troubleshooting IPv6, page 29-32
Related Topics, page 29-32

Configuration Checklist for IPv6

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

Use this information in conjunction with the document, Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x), which provides design guidelines for deploying IPv6 in your Cisco Unified Communications network.

Table 29-1 provides a checklist for configuring IPv6 in your network. Use Table 29-1 in conjunction with the “Related Topics” section on page 29-32.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Before you configure IPv6, review all IPv6-related documentation. For example, review the following documents:</td>
</tr>
<tr>
<td></td>
<td>- Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)</td>
</tr>
<tr>
<td></td>
<td>- Cisco IOS IPv6 Configuration Library</td>
</tr>
<tr>
<td></td>
<td>- Implementing VoIP for IPv6</td>
</tr>
<tr>
<td></td>
<td>- This IPv6 chapter</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Make sure that you have compatible network hardware and Cisco IOS software that is installed and configured; for example, configure your gateways and Cisco IOS MTP for IPv6. Implementing VoIP for IPv6</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS Media Termination Point Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Media Termination Points, page 29-12</td>
</tr>
</tbody>
</table>
Table 29-1   IPv6 Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> Provision a local IPv6-capable DNS and DHCP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Caution</strong> You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> Cisco recommends that the Cisco Unified Communications Manager server use a static non-link-local IPv6 address. If the Cisco Unified Communications Manager server obtains the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration, ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address from the DHCPv6 server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Install Cisco Unified Communications Manager 8.0 (or upgrade to this release).</td>
<td></td>
</tr>
<tr>
<td><strong>Caution</strong> You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> Before you install subsequent nodes (subscribers) in the cluster, add the IPv4 server information to the Server Configuration window in Cisco Unified Communications Manager Administration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Enable IPv6 in the Cisco Unified Communications Operating System and ensure that the Cisco Unified Communications Manager server obtains an IPv6 address.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> For each server in the cluster, perform these tasks. Performing these tasks requires a reboot of the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Caution</strong> You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.</td>
<td></td>
</tr>
</tbody>
</table>

Cisco recommends that the Cisco Unified Communications Manager server use a static non-link-local IPv6 address. If the Cisco Unified Communications Manager server obtains the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration, ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address from the DHCPv6 server.

Cisco Unified Communications Manager installation or upgrade 8.0 documentation
Server Configuration Settings, Cisco Unified Communications Manager Administration Guide

Cisco Unified Communications Manager, page 29-6
Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 29-21

You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.
## Configuration Checklist for IPv6 (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>In the Enterprise Parameters Configuration window in Cisco Unified Communications Manager Administration, choose <strong>True</strong> for the Enable IPv6 enterprise parameter.</td>
<td>Configuring Service and Enterprise Parameters for IPv6, page 29-25</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td></td>
</tr>
<tr>
<td>After you update this enterprise parameter, restart the Cisco CallManager, CTIManager and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>For the server that you are configuring in Cisco Unified Communications Manager Administration, choose <strong>System &gt; Server</strong> and enter the non-link-local IPv6 address or a host name that can resolve to a IPv6 address in the IPv6 Name field.</td>
<td>Server Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td></td>
</tr>
<tr>
<td>For each server in the cluster, perform this task.</td>
<td>Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration, page 29-27</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td></td>
</tr>
<tr>
<td>Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information.</td>
<td></td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td></td>
</tr>
<tr>
<td>You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for IPv6 for Cisco Unified Communications Manager until after you upgrade to Release 8.5(1). Configuring the DNS records for IPv6 for Cisco Unified Communications Manager prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.</td>
<td></td>
</tr>
<tr>
<td>To display the non-link-local IPv6 address, you can run a CLI command or view it in the Ethernet IPv6 window, as described in the “Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window” section on page 29-21.</td>
<td></td>
</tr>
</tbody>
</table>
CTI Applications

CTI provides IP address information through the JTAPI and TAPI interfaces, which can support IPv4 and IPv6 addresses. To support IPv6, applications need to use a JTAPI/TAPI client interface version that supports IPv6. Consider the following information for CTI applications and CTI port/route points:

- CTI applications connect to CTI Manager by using either an IPv4 or an IPv6 address. If you set the Enable IPv6 enterprise parameter to True in Cisco Unified Communications Manager Administration, CTI Manager can support CTI connections from applications that use IPv6 addresses.
CTI applications can register CTI ports/route points that use IPv6 or IPv4 addresses. CTI applications that handle media events for CTI ports/route points can register devices with either a IPv4 or IPv6 address, depending on the configuration for the device.

CTI applications can monitor/control CTI-supported devices that have IPv6 capability.

If a call uses IPv6, IPv6 information, including CallingPartyAddress and media IP address, gets passed to the CTI application.

### Cisco Unified Communications Manager

This section describes how Cisco Unified Communications Manager supports devices that use IPv4, IPv6, or IPv4 and IPv6. In addition, this section describes how Cisco Unified Communications Manager runs in dual-stack mode, how Cisco Unified Communications Manager can process calls for IPv4 and IPv6 devices, and how Cisco Unified Communications Manager can reserve and allocate bandwidth for IPv4 and IPv6 calls.

See the following sections:

- Cisco Unified Communications Manager Server, page 29-6
- Call Processing, page 29-7
- Call Admission Control (CAC), page 29-8

Tip

This document uses the terminology, dual stack (or dual-stack mode), which assumes that the device or server uses both an IPv4 and an IPv6 address.

### Cisco Unified Communications Manager Server

Cisco Unified Communications Manager can interact with and support devices that use IPv6 only, but you cannot configure the Cisco Unified Communications Manager server as IPv6 only because Cisco Unified Communications Manager must interact with and support devices/features that support IPv4 only (or both IPv4 and IPv6). For Cisco Unified Communications Manager to support devices that use IPv6, including dual-stack devices, which can provide both IPv4 and IPv6 addresses, you must configure Cisco Unified Communications Manager, so it runs in dual-stack mode; that is, you must ensure that the Cisco Unified Communications Manager server has both an IPv4 address and an IPv6 address that is configured for it, so it can interact and support devices that use IPv4 only, IPv6 only, or both IPv4 and IPv6.

Tip

Intracluster Cisco Unified Communications Manager node-to-node communication uses IPv4.

Before the Cisco Unified Communications Manager server can run in dual-stack mode, you must perform the following tasks:

1. On the Cisco Unified Communications Manager server, enable IPv6 in the Cisco Unified Communications Operating System.
2. Determine how the Cisco Unified Communications Manager server will get its IPv6 address, and ensure that the Cisco Unified Communications Manager server obtains its IPv6 address.

In the Cisco Unified Communications Operating System, you can request a non-link-local address from the DHCPv6 server, configure a static non-link-local IPv6 address for the Cisco Unified Communications Manager server, or obtain an non-link-local IPv6 address via stateless address autoconfiguration. (Cisco recommends a static non-link-local IPv6 address for the server.)
Ensure that the Cisco Unified Communications Manager server only obtains one non-link local IPv6 address. If the server obtains more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.

If the Cisco Unified Communications Manager server obtains an IPv6 address via stateless address autoconfiguration and you also have a static IPv6 address that is configured for the server, Cisco Unified Communications Manager ignores the IPv6 address that is obtained via stateless address autoconfiguration and uses the static address.

3. For Cisco Unified Communications Manager, set the Enable IPv6 enterprise parameter to True, which ensures that Cisco Unified Communications Manager runs in dual-stack mode. For information on this enterprise parameter, see the “Configuring Service and Enterprise Parameters for IPv6” section on page 29-25.

Caution

You must enable IPv6 in the Cisco Unified Communications Operating System and set the Enable IPv6 enterprise parameter to True. If you do not perform both of these tasks, the Cisco CallManager service runs in IPv4 and phones that you configure with an IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager.

After you perform these tasks on the server, you must restart the server for the changes to take effect.

4. In Cisco Unified Communications Manager Administration, configure the Host Name/IP Address and IPv6 Name fields in the Server Configuration window, which ensures that Cisco Unified Communications Manager runs in dual-stack mode. Cisco Unified Communications Manager considers the Host Name/IP Address field mandatory; that is, you must configure this field even if devices in your network only support IPv6. If devices in your network support IPv6 only or IPv4 and IPv6, you must configure the IPv6 Name field in addition to the IP Address/Hostname field; be aware that you must enter the non-link local IPv6 address for the Cisco Unified Communications Manager in the IPv6 Name field.

The phones use these fields, which are included in the TFTP configuration file, to retrieve the IP addresses of the Cisco Unified Communications Manager server, so phone registration occurs.

Call Processing

By running in dual-stack mode, Cisco Unified Communications Manager can set up calls under the following circumstances:

- When all devices support IPv4 only.
- When all devices support IPv6 only.
- When all devices run in dual-stack mode, in which case, Cisco Unified Communications Manager uses the configuration for the IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.
- When one device supports IPv4 and another device supports IPv6, in which case, Cisco Unified Communications Manager attempts to insert into the call an MTP that can translate IPv4 to IPv6.

Tip

Even if your device can support multiple IPv6 addresses, Cisco Unified Communications Manager only handles one IPv6 address. In addition, if your device supports an IPv4 and IPv6 address, Cisco Unified Communications Manager can simultaneously handle both addresses.
Introducing IPv6 for Cisco Unified Communications Manager

For more information on how Cisco Unified Communications Manager handles IPv4 and IPv6 calls, see the “Cisco Unified IP Phones” section on page 29-8, the “Media Termination Points” section on page 29-12, the “SIP Trunks” section on page 29-13, and the “Interactions and Restrictions” section on page 29-16.

Call Admission Control (CAC)

Because using IPv6 requires 20 more bytes of data in its header than IPv4, an IPv6 call requires more bandwidth than a similar IPv4 call that uses the same codec/media payload type. For example, a G.711 call that uses IPv4 uses 80 kb/s of bandwidth; whereas, a G.711 call that uses IPv6 uses 88 kb/s of bandwidth.

To reserve and adjust location-based bandwidth for a call that uses IPv6, Cisco Unified Communications Manager can calculate the bandwidth that is needed for an IPv6 call for all codecs that are supported with Cisco Unified Communications Manager. After the device contacts Cisco Unified Communications Manager for bandwidth reservation during the call setup, Cisco Unified Communications Manager identifies the IP version; if the call uses IPv6, Cisco Unified Communications Manager reserves the bandwidth for IPv6, and if the call uses IPv4, Cisco Unified Communications Manager reserves the bandwidth for IPv4. If Cisco Unified Communications Manager cannot identify the IP version that is used for the call, for example, the call terminates to a SIP trunk or the device supports both IP versions, Cisco Unified Communications Manager initially reserves bandwidth that supports IPv6 and later adjusts the bandwidth after media negotiation occurs.

Cisco Unified Communications Manager reserves bandwidth for one call leg at a time, so, if an MTP is inserted into the call and location-based CAC is required, ensure that the MTP is colocated with one of the devices, so location-based CAC reserves the bandwidth across the WAN based on the side that is opposite of the MTP. For example, if a call occurs from an IPv4 to IPv6 device, which causes an insertion of the MTP on the IPv4 side, Cisco Unified Communications Manager reserves bandwidth across the WAN based on IPv6. Alternatively, if the MTP is inserted for the device that uses IPv6, Cisco Unified Communications Manager reserves bandwidth across the WAN based on IPv4.

If you want to do so, you can configure the Call Counting CAC Enabled, Audio Bandwidth for Call Counting CAC, and the Video Bandwidth Unit for Call Counting CAC service parameters in Cisco Unified Communications Manager Administration, so the call uses a fixed bandwidth value instead of having Cisco Unified Communications Manager reserve and adjust bandwidth during the call. For information on these service parameters, see the “Configuring Service and Enterprise Parameters for IPv6” section on page 29-25. Be aware that configuring these service parameters can cause Cisco Unified Communications Manager to oversubscribe or undersubscribe bandwidth for the call.

Cisco Unified IP Phones

This section describes use cases for IPv4 and IPv6 calls between the phone and Cisco Unified Communications Manager. This section does not describe how the phone gets its IP address and other network settings.

For additional information on using IPv6 with your phone, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this release of Cisco Unified Communications Manager. The phone administration guide describes IPv6 settings that display on the phone.
See the following use cases, which assume that Cisco Unified Communications Manager can listen on the correct port, that an MTP is available to translate IP address versions, and that the device has the correct address version:

- Phone Has IP Addressing Mode of IPv4 Only
- Phone Has IP Addressing Mode of IPv6 Only
- Phone Has IP Addressing Mode of IPv4 and IPv6

**Tip**

Every time that the phone boots up, it boots up in dual-stack mode; that is, it can support both IPv4 and IPv6. After the phone processes the configuration file from the TFTP server, the IP Addressing Mode from the Common Device Configuration window gets set on the phone. Based on the IP Addressing Mode, the phone may disable DHCP or DHCPv6 and may release addresses that do not support the IP Addressing Mode; for example, if the IP Addressing Mode is IPv6 Only, the phone releases the IPv4 address.

If the phone has multiple, unique local or multiple global addresses, the first address that is assigned to the phone specifies the address that gets sent to Cisco Unified Communications Manager for signaling and media events. If a phone that runs in dual-stack mode loses a specific address type, the phone unregisters from Cisco Unified Communications Manager and reregisters with the remaining address type.

For media negotiation, Cisco Unified Communications Manager dynamically determines the IP address to use for the call; that is, Cisco Unified Communications Manager identifies whether the devices share the IP Addressing Mode; for example, if one device has an IP Addressing Mode of IPv4 and IPv6 and the other device has an IP Addressing Mode of IPv4 Only, Cisco Unified Communications Manager uses IPv4 for the media negotiation and requires no MTP for translating IP address versions. If the devices on the call only support one IP address version and the versions are not compatible, Cisco Unified Communications Manager uses the IP address version of the device and tries to insert an MTP into the call that can translate IPv4 to IPv6. If all devices on the call support both IP address versions, Cisco Unified Communications Manager uses the configuration for the IP Addressing Mode Preference for Media enterprise parameter for the media negotiation.

**Phone Has IP Addressing Mode of IPv4 Only**

If the IP Addressing Mode for the phone is IPv4 Only, the phone connects to Cisco Unified Communications Manager by using an IPv4 address. Signaling and media negotiation occurs by using an IPv4 address. If an IPv4 address is not available for the phone, the user cannot make calls.

**Phone Has IP Addressing Mode of IPv6 Only**

If the IP Addressing Mode for the phone is IPv6 Only and you set the Enable IPv6 enterprise parameter to True, the phone uses a global scope or unique local scope IPv6 address to connect to Cisco Unified Communications Manager. Signaling and media negotiation occur by using this IPv6 address. If an IPv6 address is not available for the phone, the user cannot make calls. Likewise, if an IPv6 address is not configured for the phone, the phone cannot register with Cisco Unified Communications Manager.
Tip
Cisco Unified Communications Manager does not support all features on phones where the IP Addressing Mode is IPv6 Only. For a list of features that are not supported, see the “Interactions and Restrictions” section on page 29-16.

If you configure IPv6 Only as the IP Addressing Mode for phones that run SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

**Phone Has IP Addressing Mode of IPv4 and IPv6**

If the IP Addressing Mode for the phone is IPv4 and IPv6 and you set the Enable IPv6 enterprise parameter to **True**, Cisco Unified Communications Manager considers the IP address support for the phone and the configuration for IP Addressing Mode Preference for Signaling setting before connecting the call.

If only one IP address version is available on the phone, the phone uses the address that is available to connect to Cisco Unified Communications Manager for signaling negotiation. If both IP addresses types are available on the phone, the phone uses the configuration for the IP Addressing Mode for Signaling setting for signaling negotiation.

**Tip**
After you configure the phone in Cisco Unified Communications Manager Administration, you can view the IP address for the phone in the Find and List Phones window. For phones that have an IPv4 address only or both IPv4 and IPv6 addresses, the IPv4 address displays in the window. For phones with an IPv6 address only, the IP Address displays as 0.0.0.0 in the IP Address column in the Find and List Phones window. To identify the IPv6 address for the phone, click the **Device Name** link in the Find and List Phones window, which causes the Phone Configuration window to display. For the IPv6 Only device, the Phone Configuration window displays an IPv4 address of 0.0.0.0, listed as IP Address, above the IPv6 address.

In the Phone Configuration window for a specific phone, you can view the IPv4 address and the IPv6 address, if applicable, that the phone uses. For phones in dual-stack mode that have both an IPv4 and IPv6 address, you can click the IPv4 or IPv6 address in the Phone Configuration window, which points to an IPv4 URL for the web server on the phone. For phones that use an IPv6 address only, you cannot click the IPv6 address because the web server on the phone only supports IPv4.

### DHCPv6

DHCPv6, which is the version of Dynamic Host Configuration Protocol that supports IPv6, can assign an IPv6 address and other network settings to the phone after you connect it to the network. In addition, DHCPv6 can assign an IPv6 address to the Cisco Unified Communications Manager server; that is, if you do not plan to assign a static IP address to the server. (Cisco recommends that you assign a static IP address to the server.)

Cisco Unified Communications Manager 7.1 does not provide DHCPv6 server capabilities, so you must configure a DHCPv6 server in your network if you plan to use DHCPv6 to assign IPv6 network configuration settings to the phone or server. If you want to allow the phone to receive its IP address via DHCPv6 rather than stateless address autoconfiguration, make sure that you set the Allow Auto-Configuration for Phones setting to Off. For information on this setting, see the “Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration” section on page 29-27.
Because Cisco Network Registrar (CNR) 6.2 provides both DNS and DHCP support for IPv4 and IPv6, consider using Cisco Network Registrar for your DNS and DHCP support. For more information on this product, see theCisco Network Registrar User’s Guide, 6.2.

If you want to do so, you can configure a Cisco IOS router or switch as a DHCPv6 server; for example, you can configure a Cisco Catalyst 3560 Series Switch or a Cisco Catalyst 3750 Series Switch that runs 12.2(46)SE (or later) as a DHCPv6 server. Before you configure this router/switch, verify that your router/switch supports the Cisco vendor-specific DHCPv6 information options that are required for IPv6 and DHCPv6 support.

For highest scope rules, consider configuring a DHCPv6 server, so it assigns only unique local addresses to the phone. If you must use global unicast addresses, configure a TLS connection and SRTP, as described in theCisco Unified Communications Manager Security Guide.

For additional information on DHCP, see the “TFTP Server” section on page 29-15, theCisco TFTP in theCisco Unified Communications Manager System Guide, andDeploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x).

DNS

For IPv6, DNSv6 handles the AAAA record, which can map IPv6 addresses. For IPv4, DNS handles the A record, which can map IPv4 addresses. For IPv4 and IPv6, the following fields rely on DNS; that is, if you configure hostnames for the fields:

- Host Name/IP Address (Server Configuration window)—You can enter an IPv4 address or host name.
- IPv6 Name (Server Configuration window)—You can enter an IPv6 address or host name.
- Destination Address (SIP Trunk Configuration window)—You can enter a valid V4 dotted IP address, a fully qualified domain name (FQDN), or DNS SRV record if the Destination Address is an SRV field is checked.
- Destination Address IPv6 (SIP Trunk Configuration window)—The allowed values for this field specify a valid IPv6 address (global unicast, unique local, or a hostname), a fully qualified domain name (FQDN), or a DNS SRV record if the Destination Address is an SRV field is checked.

You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

If the AAAA record or A record do not map correctly, calls may fail.
Introducing IPv6 for Cisco Unified Communications Manager

Because Cisco Network Registrar (CNR) 6.2 provides both DNS and DHCP support for IPv4 and IPv6, consider using CNR for your DNS and DHCP support. For more information on this product, see the Cisco Network Registrar User’s Guide, 6.2.

Gateways

MGCP and H.323 gateways do not support IPv6. To communicate with IPv6 devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.

The Cisco ATA 186 and 188 Analog Telephone Adaptors do not support IPv6.

Analog phone gateways can operate in IPv4 only, IPv6 only, or IPv4 and IPv6 (dual-stack mode).

Cisco IOS SIP gateways can support IPv6 only, IPv4 only, or IPv4 and IPv6 simultaneously in dual-stack mode. Before Cisco Unified Communications Manager can interact with these gateways, you must configure it in the SIP Trunk Configuration window in Cisco Unified Communications Manager Administration. For Cisco Unified Communications Manager considerations for the gateway, review the “SIP Trunks” section on page 29-13 and the “Media Termination Points” section on page 29-12. In addition to configuring the gateway in Cisco Unified Communications Manager Administration, you must configure the gateway, as described in Implementing VoIP for IPv6.

Media Termination Points

This section describes how Cisco Unified Communications Manager inserts MTPs into calls that require IPv4 to IPv6 translation. For information on how to configure your Cisco IOS MTP, so the MTP can support IP translation, see Implementing VoIP for IPv6.

Although the Cisco IOS MTP can support multiple IPv6 addresses, the MTP sends either a global or unique local address to Cisco Unified Communications Manager for signaling and media events.

Cisco IOS MTP supports media interoperation between IPv4 and IPv6 networks. Cisco IOS MTP for IPv4-to-IPv6 media translation operates only in dual-stack mode. In Cisco Unified Communications Manager Administration, only the Cisco IOS Enhanced Media Termination Point option for MTPs (Media Resources > Media Termination Point) and transcoders (Media Resources > Transcoder) support the translation functionality; that is, the software MTP component in the Cisco IP Voice Media Streaming Application does not support IPv4 to IPv6 translation.

When Cisco Unified Communications Manager allocates an MTP, the MTP may get used for more than one feature at the same time. Because the MTP can get used for multiple features, Cisco Unified Communications Manager prioritizes MTP allocation to ensure that IPv6 and IPv4 are supported before other features that rely on MTP get supported.
Under the following circumstances, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa):

- The devices on the call do not support the same IP address version.
- For the SIP trunk, you check the Media Termination Points Required check box or configure the Use Trusted Relay Point as On and Cisco Unified Communications Manager is communicating with devices that use IPv6 addresses. If you check the Media Termination Points Required check box for the SIP trunk or you need an MTP inserted into the call for any other reason besides IPv4 to IPv6 translation, the following considerations exist:
  - If both parties of the call can negotiate IPv4 without using an MTP, Cisco Unified Communications Manager does not insert an MTP into the call.
  - When the IP Addressing Mode is IPv6 Only or IPv4 and IPv6 for the SIP trunk, Cisco Unified Communications Manager allocates an MTP that can translate IPv4 to IPv6 (or vice versa) for the call. If no MTP that can translate IP address versions is available for the call, Cisco Unified Communications Manager allocates an MTP that supports IPv4 for the SIP trunk that is configured in dual-stack mode; for a SIP trunk that is configured as IPv6 Only, Cisco Unified Communications Manager sends an INVITE message without SDP session descriptions.

When Cisco Unified Communications Manager communicates with the MTP, Cisco Unified Communications Manager requests either an IPv4 or IPv6 address. If Cisco Unified Communications Manager requests an IPv4 address, the MTP opens an RTP port that supports IPv4. If Cisco Unified Communications Manager supports IPv6, the MTP opens an RTP port that supports IPv6.

If the request for an MTP that can translate IPv4 to IPv6 fails, the call may fail because IPv6 is required for the call. If an MTP that can translate IP address versions is inserted into the call, any intermediate media device that is inserted between the IPv6 device and the MTP must handle IPv6 requests. If Cisco Unified Communications Manager has two MTPs available and each MTP can perform only one function, Cisco Unified Communications Manager attempts to insert both MTPs into the call, the first MTP for the IPv4-to-IPv6 translation and the second MTP to support other features that require MTP. If a call requires a transcoder and an IPv6-capable MTP and the available transcoder does not support IPv6, Cisco Unified Communications Manager tries to insert the IPv6-capable MTP on the leg of the call that supports IPv6 and the transcoder on the leg of the call that supports IPv4; under these circumstances, the call fails if the IP address capabilities do not match between the MTP and transcoder.

Note

For information on specific call scenarios where SIP trunks (and MTPs) get used, see Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x).

SIP Trunks

If configured appropriately, SIP trunks can interact with devices that support IPv4 only, IPv6 only, or IPv4 and IPv6. Just like Cisco Unified Communications Manager and other components, the SIP trunk uses the configuration for the Enable IPv6 enterprise parameter to determine whether to support devices that use IPv6. See the following sections:

- IPv4 or IPv6 Signaling for SIP Trunks, page 29-14
- IPv4 or IPv6 Media for SIP Trunks, page 29-14
IPv4 or IPv6 Signaling for SIP Trunks
The following factors determine whether to use IPv4 or IPv6 for signaling events for SIP trunks:

- The direction of the call
- IP Addressing Mode for the SIP trunk, as configured in the Common Device Configuration window and applied to the trunk
- IP Addressing Mode Preference for Signaling configuration for the SIP trunk, as configured in the Common Device Configuration window (or Enterprise Parameter Configuration window) and applied to the trunk
- Configured Destination Address(es) for the SIP trunk

If you configure only one destination address, that is, either the Destination Address, which supports IPv4, or the Destination IPv6 Address, which supports IPv6, ensure that the IP Addressing Mode that you configure for the SIP trunk matches the IP address type that you configured for the destination address. If the configuration does not match, no call gets established over the trunk.

If you configure both the Destination Address and the Destination IPv6 Address, make sure that you configure the IP Addressing Mode as IPv4 and IPv6, so the trunk is in dual-stack mode. For a dual-stack trunk, the IP Addressing Mode Preference of Signaling configuration that you applied to the SIP trunk determines whether IPv4 or IPv6 gets used for signaling events for outgoing calls over SIP trunks.

IPv4 or IPv6 Media for SIP Trunks
The following factors determine whether to use IPv4 or IPv6 for media events for SIP trunks:

- The direction of the call
- Whether the call is an early offer or delayed offer call
- IP address preference in the SDP offer
- IP Addressing Mode for the SIP trunk, as configured in the Common Device Configuration window and applied to the trunk
- Configuration for the IP Addressing Mode Preference for Media enterprise parameter, as configured in the Enterprise Parameter Configuration window

For media negotiation for dual-stack devices, Cisco Unified Communications Manager dynamically determines the IP address to use for the call; that is, if any device on the call only supports one IP version, that IP version gets use, and an MTP that can translate IP versions gets inserted into the call. If all devices on the call support both IP versions, the configuration for the IP Addressing Mode Preference for Media enterprise parameter gets used.

- Configuration for the Enable ANAT check box (and whether ANAT is required or supported in the INVITE)
- IP Addressing Mode for the phone

Note
For information on specific call scenarios where SIP trunks (and MTPs) get used, see Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x).
TFTP Server

The TFTP server uses IPv4 to communicate with most components, such as the database, in Cisco Unified Communications Manager. If configured appropriately, however, the TFTP server can communicate with devices that use IPv4, IPv6, or both types of addresses.

Running in dual-stack mode, the TFTP server can respond to file requests from both IPv4 and IPv6 networks. For requests from IPv4 networks, the TFTP server responds by using an IPv4 stack; for requests from IPv6 networks, the TFTP server responds by using an IPv6 stack; that is, if you set the Enable IPv6 enterprise parameter to True.

IPv6 support applies to TFTP requests from devices and HTTP requests from off-cluster TFTP servers where the local TFTP server is configured as their alternate file server.

In an IPv6 network, the DHCPv6 server uses the Cisco vendor-specific DHCPv6 information options in the DHCPv6 response message to pass the TFTP IPv6 address to the device. If the device obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the device cannot register with Cisco Unified Communications Manager.

For more information on the Cisco vendor-specific DHCPv6 information options, see “Cisco TFTP” in the Cisco Unified Communications Manager System Guide and Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x).

The TFTP server uses the configuration for the Enable IPv6 enterprise parameter to determine how to communicate with the phone. If you set the Enable IPv6 enterprise parameter to False, the TFTP server uses IPv4 to communicate with the phone. If you set the parameter to True, the TFTP server uses IPv4 or IPv6, depending on the IP Addressing Mode for the phone. If the configuration changes for the Enable IPv6 enterprise parameter, the TFTP server receives a change notification with the new configuration, and the TFTP server enables or disables its IPv6 capabilities without requiring you to restart the Cisco TFTP service.

The configuration file that the TFTP server serves to the phone contains the configuration for the following settings:

- IP Addressing Mode, IP Addressing Mode Preference for Signaling, and Allow Auto-Configuration for the Phone
- Host Name/IP Address (IPv4 setting) for the Cisco Unified Communications Manager server
- IPv6 Name for the Cisco Unified Communications Manager server (only if you set the Enable IPv6 enterprise parameter to True)
- IPv6 address for the CAPF server (only if you set the Enable IPv6 enterprise parameter to True and activate the Cisco Certificate Authority Proxy Function service)

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service in Cisco Unified Communications Manager overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

Before the TFTP server can serve configuration files to phones that use IPv6 addresses, you must set the Enable IPv6 enterprise parameter to True. If this parameter is set to False, the TFTP server uses an IPv4 address in the configuration file, even if you configured an IP Addressing Mode of IPv6 Only for the devices.
The TFTP server obtains the IPv4 and/or IPv6 address from the Cisco Unified Communications Operating System and listens on those addresses for file requests from the phone.

In the Service Parameter Configuration window, you can also configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.

System Requirements for IPv6

The following IPv6 system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager 7.1 or later on each server in the cluster
- DHCPv6 server that can issue IPv6 addresses and DNS server that can resolve host names to IPv6 addresses; consider using Cisco Network Registrar (CNR) 6.2.
- If you want to do so, you can configure a Cisco IOS router or switch as a DHCPv6 server; for example, you can configure a Cisco Catalyst 3560 Series Switch or a Cisco Catalyst 3750 Series Switch that runs 12.2(46)SE (or later) as a DHCPv6 server. Before you configure this router/switch, verify that your router/switch supports the Cisco vendor-specific DHCPv6 information options that are required for IPv6 and DHCPv6 support.
- Cisco IOS release that is compatible with Cisco Unified Communications Manager 8.5(1), and that is installed and configured on the gateways and the Cisco IOS MTP

Tip
Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. You do not need a Cisco.com account to access Cisco Feature Navigator.

Interactions and Restrictions

Some Cisco Unified Communications Manager features do not work for devices with an IP Addressing Mode of IPv6 Only. Before you configure IPv6 Only for a device, review the following section, which describes Cisco Unified Communications Manager feature interactions and restrictions for IPv6.

Caution
You must enable IPv6 in the Cisco Unified Communications Operating System and set the Enable IPv6 enterprise parameter to True; if you do not perform both of these tasks, the Cisco CallManager service runs in IPv4, and phones that you configure with an IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager. After you perform these tasks, remember to restart the server. For the order of tasks that you perform for IPv6, see the “Configuration Checklist for IPv6” section on page 29-2.
You can provision your DNS server for IPv6 prior to performing an upgrade from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

**Annunciator**

Annunciator supports IPv4; if annunciator connects to a device with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6. If no MTP that can translate IP address versions is available, no announcement plays on the phone.

**Bulk Administration Tool**

For information on how the Bulk Administration Tool (BAT) supports IPv6, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Call Detail Records**

When IPv6 is used for a call, call detail records (CDRs) can display IPv6 addresses. For more information on CDRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

**Cisco Certificate Authority Proxy Function**

For information on how Cisco Certificate Authority Proxy Function works with IPv6, see the *Cisco Unified Communications Manager Security Guide*.

**Cisco Extension Mobility**

Cisco Extension Mobility supports IPv4, so you cannot use phones with an IP Addressing Mode of IPv6 Only for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.

**Cisco Unified Communications Manager CDR Analysis and Reporting**

For information on Cisco Unified Communications Manager CDR Analysis and Reporting, see the *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*.

**Cisco Unified Communications Operating System**

See the “Configuration Checklist for IPv6” section on page 29-2 and the “Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window” section on page 29-21.

**Cisco Unified Serviceability**

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide*.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

**Cisco Unity Connection and Cisco Unity**

Cisco Unity Connection and Cisco Unity communicate with Cisco Unified Communications Manager by using IPv4.
Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.

Real Time Monitoring Tool

In RTMT, you can monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the CTI application, CTI device, or CTI line, enter the IPv6 address, and check the AppIpv6Addr check box in the attribute window.

In addition, you can perform a device search on phones or SIP trunks that use IPv6 addresses. When you choose CallManager > Device Search > Open Device Search > Phones (or SIP Trunks), make sure that you specify an IPv6 address and check the IPv6Address check box in the attributes window.

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

In RTMT, performance monitoring counters display for the IP6 object.

Cisco Web Dialer

Cisco Web Dialer supports IPv4, so, to connect to CTI Manager, Cisco Web Dialer uses an IPv4 address. Cisco Web Dialer works with devices with an IP Addressing Mode of IPv4 and IPv6.

Conferences

Cisco Unified Communications Manager uses IPv4 for conferences, even if the conference bridge uses IPv6. During a conference, Cisco Unified Communications Manager inserts one MTP that can translate IPv4 to IPv6 for each device with an IP Addressing Mode of IPv6 Only, so each phone that uses an IPv6 address can join the conference.

For your MTP device to support security, you must configure the MTP in passthru mode, which means that the MTP does not transform the packets during the call. When you configure an MTP in passthru mode, the MTP gets the encrypted packet on one call leg and sends out the same packet on a different leg of the call. For secure conferences with secure conference bridges and encrypted devices with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP into the conference to translate IPv4 to IPv6 (and vice versa) when some devices in the conference support IPv4. If you configure the MTP for passthru mode, the encrypted IPv6 phones communicate with the conference bridge via SRTP. If you do not configure the MTP for passthru mode, the media gets downgraded to RTP.

Device Mobility

Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility.

Differentiated Services Control Point (DSCP)

Be aware that Differentiated Services Control Point (DSCP) values are the same for both IPv6 and IPv4.

Disaster Recovery System

For information on Disaster Recovery System, see the Disaster Recovery System Administration Guide.

H.323 Devices

H.323 clients, gateways, and H.225 intercluster trunks do not support IPv6. To communicate with IPv6 Only devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.
Intercom
Intercom can support phones with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. During an intercom call, the talkback mode establishes media streams with the same IP version as the media stream that is used when the caller initiated intercom.

Mobile Connect and Mobile Voice Access
Cisco Unified Mobility features in Cisco Unified Communications Manager, such as Mobile Connect and Mobile Voice Access, support IPv4. On a call, when a mobile phone uses IPv4 and another phone uses IPv6, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 into the call.

Monitoring and Recording
For monitoring and recording, the phone can handle an IPv4 media stream for customer-to-agent calls while it handles an IPv6 media stream for recording and monitoring (or vice versa).

Music On Hold
The IP Voice Media Streaming Application supports IPv4. Cisco Unified Communications Manager does not support IPv6 with multicast music on hold, so devices with an IP Addressing Mode of IPv6 Only cannot support multicast music on hold. Under these circumstances, Cisco Unified Communications Manager plays a tone, instead of music, when the phone is on hold. For IPv6 Only devices that uses unicast music on hold, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa) into the media stream.

NTP Servers
To avoid potential compatibility, accuracy, and network jitter problems, ensure that the external NTP servers that you specify for the primary node are NTP v4 (version 4).

QRT
Users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only.

RSVP
If you deploy RSVP as the call admission control mechanism in your network, do not deploy IPv6. The RSVP feature does not support IPv6. RSVP calls support IPv4. If RSVP is required for the call and any device in the call is configured for or uses an IPv6 address, Cisco Unified Communications Manager rejects the call, and the caller receives a busy tone.

SDL
SDL TCP connections support IPv6, but SDL links support IPv4. If you configure a host name in the Server Configuration window in Cisco Unified Communications Manager Administration, SDL queries the DNS A record, which ensures that IPv4 is used. If you specify an IP address, an IPv4 address gets passed down to the SDL layer.

Security (TLS and SRTP)
For information on how TLS and SRTP work with IPv6, see the Cisco Unified Communications Manager Security Guide.
SIP Phones and TFTP
Phones that run SIP do not support IPv6 addresses. If you configure IPv6 Only as the IP Addressing Mode for a phone that runs SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

T.38 Fax
Whether a T.38 fax call uses IPv4 or IPv6 depends on the preference of Cisco Unified Communications Manager and the capabilities of the devices in the call. If one device in the call uses IPv6 and the other device can use IPv4 and IPv6, the call uses IPv6, regardless of the configuration for the signaling and media enterprise parameters in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager supports the following types of T.38 fax calls:
- SIP-to-SIP call that uses IPv6
- SIP-to-SIP call that uses IPv4
- SIP-to-non-SIP call that uses IPv4
- SIP-to-non-SIP call where the SIP device uses IPv6 and the non-SIP device uses IPv4 with an MTP that can translate IP address versions

During the middle of a T.38 fax call, Cisco Unified Communications Manager does not insert an MTP that converts the IP version types; the MTP must already exist in the call.

Transfer
The transfer components in Cisco Unified Communications Manager use the IP Addressing Mode and the IP address of the device to determine how to handle the transfer. If the IP capabilities do not match when you transfer a call, Cisco Unified Communications Manager allocates an MTP that can translate IP version, so the transfer can occur.

Web Browser on the Phone
On the Cisco Unified IP Phone, the HTTP interface for the web browser supports IPv4 addresses, so the phone does not allow web access to servers that use an IPv6 address.

Video
Cisco Unified Communications Manager supports video IPv6 calls in the following cases:
- Cisco Unified Video Advantage does not support IPv6, so, when the media preference is IPv6, video uses IPv4.
- The audio and video portions of a call negotiate the same IP type for the initial call; that is, if two dual-stack phones are in a call that uses both audio and video, the call uses IPv4 for both the audio and video portions of the initial call, even when the media preference is IPv6.
- If two dual-stack phones negotiate IPv6 for the audio call based on the media preference and then you add video mid-call, the video portion of the call uses IPv4, even if the media preference is IPv6.
- MTPs do not get allocated for video support. For example, a call occurs between two dual-stack phones over a SIP trunk with an IP Addressing Mode of IPv6 Only; IPv6 gets negotiated for the audio portion of the call, and video cannot occur because the video device does not support IPv6. No MTP gets allocated to support the video portion of the call.
Installing and Activating IPv6

After you install Cisco Unified Communications Manager 7.1, your network can support IPv6 if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for IPv6” section on page 29-2.

IPv6 impacts the Cisco CallManager, CTIManager, and Certificate Authority Proxy Function services in Cisco Unified Serviceability. Depending on the configuration tasks that you perform in Cisco Unified Communications Manager Administration, you may need to restart these services after you configure IPv6.

Configuring IPv6

This section contains information on the following topics:

- Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 29-21
- Configuring Service and Enterprise Parameters for IPv6, page 29-25
- Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration, page 29-27

Tip

Before you configure IPv6, review the “Configuration Checklist for IPv6” section on page 29-2.

Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window

To enable IPv6 in the Cisco Unified Communications Operating System and to ensure that the Cisco Unified Communications Manager server gets an IPv6 address, you must perform one of the following tasks:

- Run the IPv6 CLI commands in the command line interface.
- Enable IPv6 and configure the IPv6 address in the Ethernet IPv6 window in the Cisco Unified Communications Operating System.

Caution

Before you set the Enable IPv6 enterprise parameter to True in Cisco Unified Communications Manager Administration, perform the following procedure. If you set the enterprise parameter to True before you enable IPv6 in the Cisco Unified Communications Operating System, the Cisco CallManager service runs in IPv4, and phones that have IP Addressing Mode of IPv6 Only cannot register with Cisco Unified Communications Manager.

Table 29-2 provides a description of the Ethernet IPv6 configuration settings and the equivalent CLI commands that support the graphical user interface (GUI) options.

Procedure

Step 1

In Cisco Unified Communications Operating System, choose Settings > IP > Ethernet IPv6. The Ethernet IPv6 Configuration window displays.
Step 2 To modify the Ethernet settings, enter the values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see Table 29-2.

Step 3 Check the **Update with Reboot** check box. For the IPv6 settings in this window to take effect, you must reboot the server.

Step 4 Click **Save**. The server reboots immediately after you click **Save**.

Step 5 Perform this procedure for each server in the cluster.

---

**Table 29-2 IPv6 CLI Commands and Ethernet IPv6 Configuration Settings**

<table>
<thead>
<tr>
<th>Configuration Setting in Ethernet IPv6 Window</th>
<th>Equivalent CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPv6 check box</td>
<td>set network ipv6 service enable</td>
<td>These settings enable IPv6 in the Cisco Unified Communications Operating System.</td>
</tr>
</tbody>
</table>

**Caution**
For IPv6 to work, you must either check the Ethernet IPv6 check box or issue the equivalent CLI command. You must perform this task before you set the Enable IPv6 enterprise parameter to True.
### Table 29-2  IPv6 CLI Commands and Ethernet IPv6 Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Configuration Setting in Ethernet IPv6 Window</th>
<th>Equivalent CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Advertisement radio button</td>
<td>Not applicable</td>
<td>If you want to use stateless address autoconfiguration to obtain a non-link-local IPv6 address for the Cisco Unified Communications Manager server, click the Router Advertisement radio button. Click this radio button if you do not plan to configure a static non-link-local IPv6 address for the Cisco Unified Communications Manager server or if you do not want DHCPv6 server to issue a non-link-local IPv6 address to the server. Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected. If the Cisco Unified Communications Manager server obtains an IPv6 address via stateless address autoconfiguration and you also have a static IPv6 address that is configured for the server, Cisco Unified Communications Manager ignores the IPv6 address that is obtained via stateless address autoconfiguration and uses the static address.</td>
</tr>
<tr>
<td>DHCP radio button</td>
<td>set network ipv6 dhcp enable</td>
<td>If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager server, click the DHCP radio button or issue the equivalent CLI command. Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.</td>
</tr>
</tbody>
</table>
### Table 29-2 IPv6 CLI Commands and Ethernet IPv6 Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Configuration Setting in Ethernet IPv6 Window</th>
<th>Equivalent CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Entry radio button, IPv6 Address, Subnet Mask</td>
<td>set network ipv6 static_address &lt;addr&gt; &lt;mask&gt;</td>
<td>These Ethernet IPv6 settings and equivalent CLI command allow you to configure a static IPv6 address for the Cisco Unified Communications Manager server. Configuring a static non-link-local IPv6 address assumes that you do not want the Cisco Unified Communications Manager server to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>show network ipv6 settings</td>
<td>These settings allow you to view the IPv6 address for the Cisco Unified Communications Manager server.</td>
</tr>
</tbody>
</table>

**Tip**

If you decide to run the CLI commands that are described in Table 29-2 instead of configure the Ethernet IPv6 settings in the Cisco Unified Communications Operating System, you must reboot the server for the changes to take effect. For information on how to run CLI commands and for other IPv6 CLI commands, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. 

```bash
set network ipv6 static_address <addr> <mask>
show network ipv6 settings
```
Configuring Service and Enterprise Parameters for IPv6

Table 29-3 describes the enterprise and service parameters that you can configure for IPv6. To configure enterprise parameters in Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters. To configure service parameters in Cisco Unified Communications Manager Administration, choose System > Service Parameters.

Tip

For a step-by-step procedure on how to configure enterprise parameters, see the “Enterprise Parameter Configuration” chapter in the Cisco Unified Communications Manager Administration Guide. For a step-by-step procedure on how to configure service parameters, see the “Service Parameter Configuration” in the Cisco Unified Communications Manager Administration Guide.

Table 29-3  Enterprise and Service Parameters for IPv6

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPv6</td>
<td>This enterprise parameter specifies whether Cisco Unified Communications Manager can negotiate calls by using IPv6 and whether phone can advertise an IPv6 address. Before you set this parameter to True, make sure that you enabled IPv6 in the Cisco Unified Communications Operating System on all servers in the cluster. Setting this parameter to True causes the Cisco CallManager service to run in dual-stack mode, which is required for interacting with devices that support IPv6. The default value equals False, which means that Cisco Unified Communications Manager cannot negotiate calls by using IPv6 and phones cannot advertise an IPv6 address. After you update this enterprise parameter, restart the Cisco CallManager, CTIManager, and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Media</td>
<td>This enterprise parameter, which applies only to dual-stack devices, specifies the addressing mode that Cisco Unified Communications Manager uses for media events when both IPv4 and IPv6 addresses are available from each device on the call. The default value equals Prefer IPv4.</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling</td>
<td>This enterprise parameter, which applies only to dual-stack devices, specifies how the dual-stack phone connects to Cisco Unified Communications Manager for signaling events and how the dual-stack SIP trunk connects to the peer device for signaling events. The default value equals Prefer IPv4.</td>
</tr>
<tr>
<td>Allow Auto-Configuration for Phones</td>
<td>This parameter determines whether the phone is allowed to obtain an address through stateless autoconfiguration. Valid values specify On (the phone obtains its address as specified by the router advertisements, which may be stateless or stateful, depending on the router configuration) or Off (the phone always uses DHCPv6 to obtain its IPv6 address).</td>
</tr>
</tbody>
</table>
### Table 29-3 Enterprise and Service Parameters for IPv6 (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Call Counting CAC Enabled</strong></td>
<td>This service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager uses call counting as part of the locations-based call admission control (CAC) feature. Call counting uses a fixed bandwidth value to reserve and adjust bandwidth per call, regardless of the codec or media payload or the Internet Protocol Version (IPv6 or IPv4) that is used for each call. Call counting may potentially oversubscribe or undersubscribe bandwidth because a fixed-value bandwidth gets reserved per call no matter what the actual bandwidth is for the call. Cisco recommends you leave this parameter set to the default value of False (disabled) unless your network requires the call counting feature. To enable call counting for CAC, choose True for the parameter; to disable call counting for CAC, choose False. This service parameter applies to IPv4 and IPv6 calls.</td>
</tr>
<tr>
<td><strong>Audio Bandwidth For Call Counting CAC</strong></td>
<td>This service parameter, which supports the Cisco CallManager service, specifies the amount of bandwidth to deduct from the available bandwidth for audio calls after you set the Call Counting CAC Enabled parameter to True. For each audio call, the amount of bandwidth that you enter in this field gets deducted, regardless whether more or less bandwidth is actually used for the call. This service parameter applies to IPv4 and IPv6 calls.</td>
</tr>
<tr>
<td><strong>Video Bandwidth For Call Counting CAC</strong></td>
<td>This service parameter, which supports the Cisco CallManager service, specifies the units of bandwidth to deduct from the available bandwidth for video calls after you set the Call Counting CAC Enabled parameter to True. For each video call, the available bandwidth gets reduced by the number of units that are required to account for the actual bandwidth usage. For example, if you specify 512 kb/s as the bandwidth unit in this parameter, and a video call utilizes 384 kb/s, then one unit, 512 kb/s, gets deducted from available bandwidth. Likewise, if you specify 512 kb/s in this parameter and a video call negotiated 768 kb/s, then two units of bandwidth (1064 kb/s) get deducted from the available bandwidth. This service parameter applies to IPv4 and IPv6 calls.</td>
</tr>
<tr>
<td><strong>Alternate Cisco File Server(s)</strong></td>
<td>These service parameters, which support the Cisco TFTP service, allow you to configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.</td>
</tr>
</tbody>
</table>
Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration

Table 29-4 describes the IPv6 and IPv4 settings that are in Cisco Unified Communications Manager Administration, except for IPv6 service and enterprise parameters, which are described in Table 29-3. For some IPv6 settings in Table 29-4, equivalent settings for IPv4 display in Cisco Unified Communications Manager Administration; for example, in the SIP Trunk Configuration window, you can configure the Destination Address IPv6 setting or the Destination Address setting, or both settings, depending on the IP support in your network.

For related configuration procedures, see the following sections:

- Configuring Service and Enterprise Parameters for IPv6, page 29-25
- Server Configuration Settings, Cisco Unified Communications Manager Administration Guide
- SIP Route Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Common Device Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Configuring a Trunk, Cisco Unified Communications Manager Administration Guide

Table 29-4 IPv6 Settings in Cisco Unified Communications Manager Administration

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System &gt; Server</td>
<td></td>
</tr>
<tr>
<td>Host Name/IP Address</td>
<td>This field supports IPv4. If your network uses DNS that can map to IPv4 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, you must enter the full IPv4 address of the server.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If your network supports IPv6 (or IPv4 and IPv6), configure the IPv6 Name field in addition to the Host Name/IP Address field.</td>
</tr>
</tbody>
</table>
Chapter 29  Internet Protocol Version 6 (IPv6)

### Configuring IPv6

**IPv6 Name**
This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the “Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window” section on page 29-21.

Phones that run SCCP use this field, which gets included in the TFTP configuration file, to retrieve the IPv6 address of the Cisco Unified Communications Manager server, so phone registration occurs.

**Tip**
You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

**Tip**
In addition to configuring the IPv6 Name field, you must configure the Host Name/IP Address field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).

### Call Routing > SIP Route Patterns

**IPv4 Pattern**
Enter the domain, sub-domain, IPv4 address or IP subnetwork address.

**Tip**
For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, enter X.X.X/X/Y, where Y equals the network prefix that denotes the number of bits in the address that will be the network address.

**Tip**
If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.

**IPv6 Pattern**
Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6.

**Tip**
If the SIP trunk supports both IPv4 and IPv6, configure the IPv4 Pattern in addition to the IPv6 Pattern.

---

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Name</td>
<td>This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the “Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window” section on page 29-21. Phones that run SCCP use this field, which gets included in the TFTP configuration file, to retrieve the IPv6 address of the Cisco Unified Communications Manager server, so phone registration occurs. <strong>Tip</strong> You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(x) to Release 8.5(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 8.5(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.5(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. <strong>Tip</strong> In addition to configuring the IPv6 Name field, you must configure the Host Name/IP Address field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).</td>
</tr>
<tr>
<td>Call Routing &gt; SIP Route Patterns</td>
<td></td>
</tr>
<tr>
<td>IPv4 Pattern</td>
<td>Enter the domain, sub-domain, IPv4 address or IP subnetwork address. <strong>Tip</strong> For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, enter X.X.X/X/Y, where Y equals the network prefix that denotes the number of bits in the address that will be the network address. <strong>Tip</strong> If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv6 Pattern in addition to the IPv4 pattern.</td>
</tr>
<tr>
<td>IPv6 Pattern</td>
<td>Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. <strong>Tip</strong> If the SIP trunk supports both IPv4 and IPv6, configure the IPv4 Pattern in addition to the IPv6 Pattern.</td>
</tr>
</tbody>
</table>
### Configuring IPv6

Device > Device Settings > Common Device Configuration

**IP Addressing Mode**
Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to Cisco Unified Communications Manager. From the drop-down list box, choose one of the following options:

- **IPv4 Only**—For both media and signaling events, the device uses an IPv4 address to connect to Cisco Unified Communications Manager. If an IPv4 address is not available for the device, the call fails.

  If you choose this option, the phone releases an IPv6 address. If you choose this option, the SIP trunk uses an IPv4 address to connect to the peer device.

- **IPv6 Only**—For both media and signaling events, the device uses an IPv6 address to connect to Cisco Unified Communications Manager. If an IPv6 address is not available for the device, the call fails.

  If you choose this option, the phone releases an IPv6 address. If you choose this option, the SIP trunk uses an IPv6 address to connect to the peer device.

  Phones that run SIP do not support IPv6, so do not choose this option for these phones. If you configure IPv6 Only as the IP Addressing Mode for phones that run SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

- **IPv4 and IPv6 (Default)**—Choose this option for dual-stack devices, which can have both an IPv4 and IPv6 address. For both media and signaling events, the dual-stack device uses either an IPv4 or an IPv6 address to connect to Cisco Unified Communications Manager.

  If only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call.

  If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.

**IP Addressing Mode Preference for Signaling**
For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events.

From the drop-down list box, choose one of the following options:

- **IPv4**—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event.

- **IPv6**—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event.

- **Use System Default**—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.
### Configuring IPv6

**Allow Auto-Configuration for Phones**

This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options:

- **On**—Depending on how the M bit is set via stateless address autoconfiguration on the router, the phone is allowed to use the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address.

  Phones also require a TFTP server address to register with Cisco Unified Communications Manager. You can manually configure the TFTP server address via the interface on the phone, or you can obtain it from a DHCPv6 server.

  **Tip**
  To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O bit is set via stateless address autoconfiguration on the router.

- **Off**—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server.

- **Default**—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.

Although Cisco Unified Communications Manager does not use this configuration, the TFTP file that the phone obtains includes this information.

### Device > SIP Trunk

**Destination Address**

The Destination Address, which supports IPv4, represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid V4 dotted IP address, fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked.

SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.

If the remote end is a Cisco Unified Communications Manager cluster, DNS SRV represents the recommended choice for this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.

**Tip**

For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual-stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.
Chapter 29  Internet Protocol Version 6 (IPv6)

Configuring IPv6

Table 29-4  IPV6 Settings in Cisco Unified Communications Manager Administration (continued)

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination Address IPv6 | The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. Enter one for the following values in the field:  
  • A valid IPv6 address (global unicast, unique local, or a host name)  
  • A fully qualified domain name (FQDN)  
  • A DNS SRV record, but only if you check the Destination Address is an SRV check box.  
  
  SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.  
  
  If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. |
| Enable ANAT | This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media.  
  
  When you check both the Enable ANAT and the Media Termination Point Required check boxes, Cisco Unified Communications Manager inserts a dual-stack MTP and sends out an offer with two m-lines, one for IPv4 and another for IPv6. If a dual-stack MTP cannot be allocated, Cisco Unified Communications Manager sends an INVITE without SDP.  
  
  When you check the Enable ANAT check box and the Media Termination Point Required check box is unchecked, Cisco Unified Communications Manager sends an INVITE without SDP.  
  
  When both the Enable ANAT and Media Termination Point Required check boxes display as unchecked (or when an MTP cannot be allocated), Cisco Unified Communications Manager sends an INVITE without SDP.  
  
  When you uncheck the Enable ANAT check box but you check the Media Termination Point Required check box, consider the information, which assumes that an MTP can be allocated:  
  
    •  
    - Cisco Unified Communications Manager sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only.  
    
    •  
    - Cisco Unified Communications Manager sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only.  
    
    •  
    - For dual-stack SIP trunks, Cisco Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter. |
Providing Information to End Users

No special considerations exist for phone (end) users, although IPv6 menu options display on the phone. Be aware, though, that if you do not configure the IP address support correctly in your network, users may receive a busy tone, dead air, and so on, when trying to place or answer calls on the phone.

For additional information on using IPv6 with your phone, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this version of Cisco Unified Communications Manager.

Troubleshooting IPv6

For information on troubleshooting IPv6, see the Cisco Unified Communications Manager Troubleshooting Guide.

Related Topics

- Configuration Checklist for IPv6, page 29-2
- Introducing IPv6 for Cisco Unified Communications Manager, page 29-5
- Running IPv6 CLI Commands or Configuring IPv6 in the Ethernet IPv6 Window, page 29-21
- Configuring Service and Enterprise Parameters for IPv6, page 29-25
- Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified Communications Manager Administration, page 29-27
- Server Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco IOS Media Termination Point Configuration Settings, Cisco Unified Communications Manager Administration Guide
- SIP Route Pattern Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Configuring a Trunk, Cisco Unified Communications Manager Administration Guide
- Common Device Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Cisco TFTP, Cisco Unified Communications Manager System Guide

Additional Cisco Documentation

- Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)
- Cisco Unified IP Phone Administration Guide
- Cisco IOS IPv6 Configuration Library
- Implementing VoIP for IPv6
Related Topics

- Cisco Network Registrar User's Guide, 6.2
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Call Detail Records Administration Guide
- Cisco Unified Communications Manager Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide
- Cisco Unified Communications Operating System Administration Guide
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
Licensing

Use licensing in Cisco Unified Communications Manager Administration to accurately track the number of devices that are connected to Cisco Unified Communications Manager, including third-party phones that run SIP, and compare it with the number of unit licenses that have been purchased.

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of devices.

Licenses get generated for requested Cisco Unified Communications Manager nodes (servers in a Cisco Unified Communications Manager cluster) and the devices that are associated with those nodes. Two types of licenses exist: production licenses and starter licenses. Production licenses for Cisco Unified Communications Manager comprise licenses for devices and nodes that are purchased from Cisco. License device types include physical devices such as IP phones and applications such as IP communicator.

New installations of Cisco Unified Communications Manager include starter licenses that get replaced when a production license file gets uploaded. Cisco does not provide starter licenses for upgrades or migrations.

This section covers the following topics:

- Checklist for Licensing, page 30-2
- Licensing for Cisco Unified Communications Manager on VMware on Cisco UCS B-Series Blade Servers, page 30-3
- Understanding Licensing, page 30-3
  - Understanding Licensing Terminology, page 30-3
  - Understanding Licensing-Related Windows, page 30-4
  - Understanding the Contents of the License File, page 30-6
  - Understanding How Licensing Works for Phones, page 30-8
  - Understanding How Adjunct Licensing Works, page 30-9
  - Understanding How Licensing Works for Applications, page 30-9
- Interactions and Restrictions, page 30-11
- Working with Licenses, page 30-12
  - Calculating the Number of Required License Units, page 30-12
  - Obtaining a License File, page 30-13
  - Verifying That the License Manager Service Is Running, page 30-15
  - Uploading a License File, page 30-16
Checklist for Licensing

Table 30-1 describes steps for licensing if you are installing or upgrading a server.

### Checklist for Licensing

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Review the documentation on licensing.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Determine the number of licenses and device license units that you need for your Cisco Unified Communications Manager system.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Obtain the license(s).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Install or upgrade the servers in the cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Upload the license in Cisco Unified Communications Manager Administration. (System &gt; Licensing &gt; License File Upload)</td>
</tr>
<tr>
<td>Step 6</td>
<td>After you upload the license, verify that the Cisco CallManager service is running on all nodes where it had previously been activated. If it is not running, restart the service. (Tools &gt; Control Center—Feature Services)</td>
</tr>
</tbody>
</table>
Licensing for Cisco Unified Communications Manager on VMware on Cisco UCS B-Series Blade Servers

For information about licensing for Cisco Unified Communications Manager on VMware on Cisco UCS B-Series Blade Servers, see the document *Installing Cisco Unified Communications Manager*.

Understanding Licensing

Use licensing in Cisco Unified Communications Manager Administration to accurately track the number of devices that are connected to Cisco Unified Communications Manager, including third-party phones that run SIP, and compare it with the number of unit licenses that have been purchased.

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of devices.

Licenses get generated for requested Cisco Unified Communications Manager nodes (servers in a Cisco Unified Communications Manager cluster) and the devices that are associated with those nodes.

Understanding Licensing Terminology

Table 30-2 describes common terminology that is used for licensing.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjunct Licensing/Adjunct Device</td>
<td>With adjunct licensing, fewer device license units (DLUs) get consumed for adjunct (secondary) devices, such as Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, when these applications get used with a Cisco Unified IP Phone, which serves as the primary device. For adjunct licensing to work, the adjunct device must consume fewer or the same number of DLUs as the primary device.</td>
</tr>
<tr>
<td>Device License Unit (DLU)</td>
<td>Device license units are assigned to each device that is connected to Cisco Unified Communications Manager. Each device is assigned a unit number based on the type and capabilities of the device. Devices with more complex and high-end capabilities are assigned a higher number of units.</td>
</tr>
</tbody>
</table>
Chapter 30  Licensing

Understanding Licensing

The configuration windows in Table 30-3 support licensing in Cisco Unified Communications Manager Administration:

### Table 30-2 Licensing Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Authorization Key (PAK)</td>
<td>When you place an order for Cisco devices, Cisco provides a Product Authorization Key (PAK). Using PAK, you can split the licenses across multiple clusters when over 1,000 device license unit bundles are purchased. For example, you request 20 Cisco Unified Communications Manager nodes and 20000 phone units in one purchase order. A PAK gets issued after the request is approved. Using this PAK, you can split the licenses across multiple clusters with 1 license file containing 15 Cisco Unified Communications Manager nodes and 15000 phone units and another license file with 5 Cisco Unified Communications Manager nodes and 5000 phone units.</td>
</tr>
<tr>
<td>Production License</td>
<td>Production licenses for Cisco Unified Communications Manager comprise licenses for devices and nodes that are purchased from Cisco.</td>
</tr>
<tr>
<td>Starter License (also called demo license)</td>
<td>Cisco Unified Communications Manager contains a starter license that you can use to begin new installations of Cisco Unified Communications Manager before you install the production license. Starter licenses, which are available in limited quantities, have no expiration date. You can use starter licenses only for fresh installations; you cannot use them for upgrades or migrations from previous releases. Starter licenses support only one Cisco Unified Communications Manager node and up to 50 device license units. The system overwrites the starter licence when you obtain and upload your production licenses.</td>
</tr>
</tbody>
</table>

**Understanding Licensing-Related Windows**

The configuration windows in Table 30-3 support licensing in Cisco Unified Communications Manager Administration:
Table 30-3  Licensing Windows in Cisco Unified Communications Manager Administration

<table>
<thead>
<tr>
<th>Window</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main window</td>
<td>After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For example, Cisco Unified Communications Manager may identify the following situations:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager currently operates with starter licenses, so upload the appropriate license files.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager currently operates with an insufficient number of licenses, so upload additional license files.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager does not currently use the correct software feature license. In this case, the Cisco CallManager service stops and does not start until you upload the appropriate software version license and restart the Cisco CallManager service.</td>
</tr>
<tr>
<td>System &gt; Licensing &gt; License Unit Report</td>
<td>This window displays the total license capacity and the number of licenses in use. Cisco Unified Communications Manager generates a report that lists the total number of available licenses. The license unit report also displays the software license version that is installed on the Cisco Unified Communications Manager server. This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, Invalid, or Uploaded.</td>
</tr>
<tr>
<td>System &gt; Licensing &gt; License Unit Calculator</td>
<td>This window allows you to calculate the number of device license units that are required for a phone model or application.</td>
</tr>
<tr>
<td>System &gt; Licensing &gt; License File Upload</td>
<td>This window allows you to upload the license file that you obtained. In addition, this window displays a message that uploading the license file removes the starter licenses for the feature. You can also view the license file from this window.</td>
</tr>
<tr>
<td>System &gt; Licensing &gt; Capabilities Assignment</td>
<td>This window triggers licensing to consume device license units for Cisco Unified Presence (CUP) and Cisco Unified Personal Communicator (CUPC) users.</td>
</tr>
<tr>
<td>User Management &gt; End User</td>
<td>This window displays the Enable Mobility check box, which triggers licensing to consume device license units for Cisco Unified Mobility. For more information, see the “Licenses for Cisco Unified Mobility” section on page 30-9.</td>
</tr>
<tr>
<td>Device &gt; Phone</td>
<td>This window displays the Device Is Active message, which triggers licensing to consume device license units for the phone. This window displays the Primary Phone drop-down list box for Cisco IP Communicator, Cisco Unified Mobile Communicator, Cisco Unified Personal Communicator, and Client Services Framework. Configuring the Primary Phone setting triggers licensing to consume fewer device license units for the application because it serves as an adjunct device, not the primary device.</td>
</tr>
</tbody>
</table>
Understanding Licensing

Chapter 30      Licensing

Understanding the Contents of the License File

The license file, which you can view from the License File Upload window, contains the following information:

- Number of Cisco Unified Communications Manager nodes that are licensed—This indicates number of Cisco Unified Communications Manager servers in a cluster that are licensed to the customer.
- Versions of the Cisco Unified Communications Manager that are supported.
- Number of phone units that are licensed—Instead of creating a separate license for each phone type, the system uses the concept of license units. Each phone type corresponds to a fixed number of license units.

Note To determine the number of license units that are required for each device, choose System > Licensing > License Unit Calculator. This window lists the number of license units that are required for each type of device.

- MAC address of the server, where the license file can be installed.

Sample License Files

The following examples (Example 30-1, Example 30-2, Example 30-3), respectively, describe license files for permanent IP phone licenses, permanent Cisco Unified Communications Manager node licenses, and software feature licenses.

Example 30-1 Permanen t IP Phone Licenses

INCREMENT PHONE_UNIT cisco 6.0 permanent uncounted \\
VENDOR_STRING=<Count>1000</Count><OrigMacId>00BCD4EE59D</OrigMacId><LicFileVersion>1.0</LicFileVersion> \\
HOSTID=00bcd4ee59d OVERDRAFT=50 \\
NOTICE="<LicFileID>20050826140539162</LicFileID><LicLineID>2</LicLineID> \\
<PAT></PAT>" SIGN="112D 17E4 A755 5EDC F616 0F2B B820 A89C \\
0313 A36F B317 F359 18E8 5E15 ES24 1915 66EA BC9F A82B CBC8 \\
4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B"

The preceding license file includes following information:

- No expiration date for this license exists as indicated by the keyword permanent.
- This license file provides 1000 PHONE_UNIT licenses.
- OVERDRAFT=50 indicates (5 percent of 1000) allowed overdraft. Cisco determines the overdraft value.
- The Cisco-specific fieldLicFileID identifies this license file.
- You can add multiple increment lines for same feature (phone unit license or node license) in a license file to increase the license count. Identical INCREMENT lines should not exist, and each line should be signed independently.
- To use 5.0 device licenses with Cisco Unified Communications Manager 6.0(1) or later, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.
Example 30-2  Permanent CCM_Node licenses

INCREMENT CCM_NODE cisco 6.0 permanent uncounted \ 
VENDOR_STRING=<Count>2</Count><OrigMacId>000e7feeebbd</OrigMacId><LicFileVersion>1.0</LicFileVersion> \ 
HOSTID=000e7feeebbd \ 
NOTICE="<LicFileID>20060309193216861</LicFileID><LicLineID>1</LicLineID> 
<PAK></PAK>" SIGN="1375 87CA 021E 6ABD C2EF C1D2 1E1A 9A08 
6A0C 6624 1F21 E5CC 8D83 E154 202F 0A2A 4F75 00D6 C102 E5B9 
5DA2 A3F9 AE3B CD9A CC86 3F14 9455 28F9 CBC8 31CC"

The preceding license file includes the following information:

- No expiration date for this license exists as indicated by the keyword permanent. Permanent indicates that the license file is not temporary. A temporary license would have a date here instead.
- This license file provides two licenses for the version 5.0 of the feature CCM_NODES.
- Original MAC ID specifies the MAC ID for which license file was first issued.
- HOST ID specifies the MAC ID of the publisher server. This would differ from the OrigMacID only if a rehost procedure was done for the license file.
- The Cisco specific fieldLicFileID identifies this license file.
- SIGN represents the signature that FlexLM generates, and the FlexLM validation package uses it in Cisco Unified Communications Manager to detect whether license file tampering occurred.
- You can add multiple increment lines for same feature in a license file to increase the license count. Ensure that none of the INCREMENT lines is identical, and ensure that each of them is signed independently.

Example 30-3  Software Feature licenses

INCREMENT SW_FEATURE cisco 6.0 permanent uncounted \ 
VENDOR_STRING=<Count>1</Count><OrigMacId>111222333444</OrigMacId><LicFileVersion>1.0</LicFileVersion> \ 
HOSTID=111222333444 \ 
NOTICE="<LicFileID>20070911134257196</LicFileID><LicLineID>1</LicLineID> 
<PAK></PAK>" SIGN="15CF FEF2 BB28 3A61 014F AEC1 7F18 8F8D 
6EC8 7BA7 8ACB 0267 BA3A DE1D BF04 0230 96A8 6D6A 83B6 D0CC \ 
1E53 E091 1304 924E C7A3 CCEB 12E6 6FA3 E95C 6C92"

The preceding license file includes the following information:

- No expiration date for this license exists as indicated by the keyword permanent.
- The INCREMENT SW_FEATURE line indicates that this license provides feature support for Cisco Unified Communications Manager 6.0.
- To use 5.0 device licenses with Cisco Unified Communications Manager 6.0(1) or later, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.
Understanding How Licensing Works for Phones

Each phone type requires a fixed number of device license units. For example, Cisco Unified IP Wireless Phone 7920 requires four device license units, and Cisco Unified IP Phone 7970 requires five device license units. If you want licenses for four 7920 phones and four 7970 phones, you require 36 device license units.

Before you configure a phone in the Phone Configuration window, consider the following information:

- If the Cisco Unified Communications Manager database contains a real MAC address for a phone, not the dummy MAC address that is created via the Bulk Administration Tool (BAT), licensing immediately consumes device license units for the phone after the phone gets added to the database.
  - If the number of used device license units and number of pending device licensing units do not exceed the total number of device license units that are available for use, the phone with the real MAC address gets added to the database.
  - If the number of used device license units and number of pending device licensing units exceed the total number of device license units that are available for use, the phone with the real MAC address does not get added to the database.

- The Device Is Active message in the Phone Configuration window in Cisco Unified Communications Manager Administration displays when a phone consumes device license units and when a phone can register with Cisco Unified Communications Manager.
  - For a phone that uses a real MAC address, not the dummy MAC address that is created via BAT, the Device Is Active message displays, which indicates that the phone uses device license units and can register with Cisco Unified Communications Manager.
  - For a phone that uses the dummy MAC address that is created via BAT, the Device Is Active message does not display. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, the Device Is Active message displays after you save the configuration; this ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone.

- Cisco Unified Communications Manager allows you to provision phones with dummy MAC addresses via BAT as long as the number of used device license units and the number of pending device license units do not exceed the total number of device license units that are available for use.

- If you use the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS) to associate an auto-registered phone with the BAT dummy settings, the Cisco Unified Communications Manager Auto-Register Phone Tool deletes the auto-registered phone from the database, and licensing gives you credits for the device license units for the deleted phone. After the Cisco Unified Communications Manager Auto-Register Phone Tool applies the device name to the phone that uses the dummy MAC address, the Device Is Active message displays in Phone Configuration window. Licensing consumes device license units for the phone, and the phone can register with Cisco Unified Communications Manager, unless the number of used device license units exceeds the total number of device license units that are available for use.

- When a phone auto-registers for use with the Cisco Unified Communications Manager Auto-Register Phone Tool, it gets inserted into the database as long as the number of used device license units is less than the number of device license units that are available for use.

- You can view the number of pending, used, and available device license units in the License Unit Report and the License Unit Calculator in Cisco Unified Communications Manager Administration.
Understanding How Adjunct Licensing Works

With adjunct licensing, fewer device license units (DLUs) get consumed for adjunct (secondary) devices, such as Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator, when these applications get used with a Cisco Unified IP Phone, which serves as the primary device. For adjunct licensing to work, the adjunct device must consume fewer or the same number of DLUs as the primary device.

For example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7970, Cisco IP Communicator consumes only one DLU. Adjunct licensing works because the Cisco Unified IP Phone 7970 consumes five DLUs and Cisco IP Communicator consumes three DLUs.

In another example, if you configure Cisco IP Communicator as a secondary device for the Cisco Unified IP Phone 7906, adjunct licensing fails because the Cisco Unified IP Phone 7906 consumes two DLUs and Cisco IP Communicator consumes three DLUs. An error occurs when you configure an application, for example, Cisco IP Communicator, as the adjunct device, and the adjunct device requires more device license units (DLUs) than the primary device; for example, the Cisco Unified IP Phone 7906.

To ensure that Cisco Unified Communications Manager treats Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator as adjunct (secondary) devices, configure the Primary Phone setting in the Phone Configuration window for Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator.

The License Unit Calculator window displays (Adjunct) next to the applications that work as adjunct devices.

Understanding How Licensing Works for Applications

Certain types of applications, such as Cisco IP Communicator, consume device license units as primary devices or adjunct devices, which are devices or applications that an end user uses in addition to the desktop phone; for example, Cisco IP Communicator becomes an adjunct device when the end user uses both the desktop phone and Cisco IP Communicator. Cisco IP Communicator becomes the primary device when the end user does not use a desktop phone.

For specific information on licensing for specific applications, see the following sections:

- Licenses for Cisco IP Communicator, page 30-9
- Licenses for Cisco Unified Mobility, page 30-9
- Licenses for Cisco Unified Mobile Communicator, page 30-10
- Licenses for Cisco Unified Personal Communicator, page 30-10

Licenses for Cisco IP Communicator

If Cisco IP Communicator gets configured as a primary device for an end user, it consumes three device license units. If it gets configured as an adjunct device (by choosing a phone in the Primary Phone field in Phone Configuration), it consumes one device license unit.

Licenses for Cisco Unified Mobility

Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units for Mobile Connect. The number of device license units that are consumed depends on whether you assign the end user an adjunct device, that is, a desktop phone, for example, specifically for Cisco Unified Mobility. You assign the end user an adjunct device for Cisco Unified
Understanding Licensing

Before you enable Mobile Connect, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to assign the same device for Cisco Unified Mobility to multiple users.
- When you plan your configuration, determine whether the user uses both a desktop phone and a cell phone. If the user uses both a cell phone and a desktop phone, make sure that you assign an adjunct device to the user after you enable Mobile Connect in the End User Configuration window.
  
  The device that you assign serves as the adjunct device; that is, the device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility.
- If you enable Mobile Connect and fail to assign the end user an adjunct device for Cisco Unified Mobility, four DLUs get consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.
- If you enable Mobile Connect and assign the end user an adjunct device for Cisco Unified Mobility, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the License Unit Calculator window.
- If you enable Mobile Connect and later decide to assign an adjunct device for the feature to the end user, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.
  
  For example, if you enable Mobile Connect, forget to assign the end user an adjunct device for the feature, and click **Save**, the system consumes four DLUs. If you then assign the end user an adjunct device for the feature and click **Save**, the system credits you with two DLUs.
- If you delete the device from Cisco Unified Communications Manager Administration or remove the assignment after you enable Mobile Connect, two DLUs get consumed after you delete the device or remove the assignment, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.

**Licenses for Cisco Unified Mobile Communicator**

Cisco Unified Mobile Communicator uses one Device License Unit (DLU) if the user has a desktop phone and three DLUs if the user does not have a desktop phone; that is, if the user uses Cisco Unified Mobile Communicator as the primary device. When you configure the Cisco Unified Mobile Communicator in the Phone Configuration window, choose a primary phone from the Primary Phone drop-down list box if Cisco Unified Mobile Communicator is the adjunct (secondary) device.

**Licenses for Client Services Framework**

When you configure Client Services Framework in the Phone Configuration window, choose a primary phone from the Primary Phone drop-down list box if Client Services Framework is the adjunct (secondary) device.

**Licenses for Cisco Unified Personal Communicator**

Configuring the License Capabilities Assignments settings in Cisco Unified Communications Manager Administration triggers licensing to consume device license units for Cisco Unified Personal Communicator. See the “License Capabilities Assignment Configuration Settings” section on page 30-18.
Interactions and Restrictions

The following interactions and restrictions exist for licensing:

- Cisco strongly recommends that you obtain the license by using Microsoft Outlook as your email client. Using other email clients to obtain the license file may cause additional characters to display in the license file.

- Before you upload a license file in Cisco Unified Communications Manager Administration, verify in Cisco Unified Serviceability that the Cisco License Manager service is running.

  The license manager service keeps track of the licenses that get purchased and used. It refers to the processes that control the checkin and checkout of the licenses, and it keeps track of the number of license units that are required for each phone and application type. The license manager has responsibility for issuing and reclaiming licenses and for detecting whether an overdraft of licenses occurs.

- You do not need to obtain new licenses if you are upgrading within a software release train, such as Cisco Unified Communications Manager 6.0(1) to 6.1(1).

- After some upgrades to 8.5(1), the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated. Immediately after you complete the upgrade to Cisco Unified Communications Manager 8.5(1), upload the software feature license that is required for Cisco Unified Communications Manager 8.5(1) in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 8.5(1).

- After you upload the license file, you must restart the Cisco CallManager service in Cisco Unified Serviceability.

- Cisco Unified Communications Manager keeps track of the software license version. Each time that the Cisco CallManager service restarts, this version check gets performed. If Cisco Unified Communications Manager fails to load (for example, because the license file is missing), the Service Manager tries to restart the Cisco CallManager service three times. At each attempt to restart, the license file check gets performed, and an alarm gets written to syslog.

  The software license version displays in the License Unit Report window of Cisco Unified Communications Manager Administration.

- The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

- For DNS, make sure that you map the IP addresses of all servers, including dummy nodes, to the hostnames on the DNS server. If you do not perform this task, Cisco Unified Communications Manager generates alarms that the License Manager service is down.

- You cannot delete a license file name through Cisco Unified Communications Manager Administration. For information on how to delete a license file name, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

- The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.
Working with Licenses

This section contains information on the following topics:

- Calculating the Number of Required License Units, page 30-12
- Obtaining a License File, page 30-13
- Verifying That the License Manager Service Is Running, page 30-15
- Uploading a License File, page 30-16
- Generating a License Unit Report, page 30-17
- License Capabilities Assignment Configuration Settings, page 30-18
- Finding a License Capabilities Assignment, page 30-19
- Configuring the Capabilities Assignments for One User, page 30-20
- Configuring the Capabilities Assignments for Multiple Users, page 30-20
- Alarms, Alerts, and License Status Notification, page 30-21

Calculating the Number of Required License Units

When you place an order for Cisco devices, Cisco provides a Product Authorization Key (PAK). Using PAK, you can split the licenses across multiple clusters when over 1,000 device license unit bundles are purchased.

For example, you request 20 Cisco Unified Communications Manager nodes and 20000 phone units in one purchase order. A PAK gets issued after the request is approved. Using this PAK, you can split the licenses across multiple clusters with 1 license file containing 15 Cisco Unified Communications Manager nodes and 15000 phone units and another license file with 5 Cisco Unified Communications Manager nodes and 5000 phone units.

To determine the number of license units that are required for each device after you install or upgrade Cisco Unified Communications Manager, choose System > Licensing > License Unit Calculator in Cisco Unified Communications Manager Administration. Use the License Unit Calculator window to calculate the number of phone unit licenses that are required for a specific configuration of a type of phones and number of phones of each type. A device license unit refers to a fixed number of license units that corresponds to each phone type. Cisco Unified IP Wireless Phone 7920 requires four license units, and a Cisco Unified IP Phone 7970 requires five units. If you are adding four 7920 phones and four 7970 phones, you require 36 phone license units.

Table 30-4 provides an example of how Cisco Unified Communications Manager performs the calculations for primary and adjunct license units.
Use the following procedure to calculate the number of phone licenses that are required when the number of phone types and the total number of phones per phone type are entered.

**Procedure**

**Step 1** Choose System > Licensing > License Unit Calculator.

The License Unit Calculator window displays. The number of license units that are consumed per device displays, corresponding to the node or device.

**Step 2** In the Number of Devices column, update the number of needed devices, corresponding to each node or phone.

**Step 3** Click Calculate.

The total number of Cisco Unified Communications Manager node license units and phone license units displays.

**Additional Information**

See the “Related Topics” section on page 30-22.

### Obtaining a License File

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of devices. This section provides information on obtaining licenses for new Cisco Unified Communications Manager systems and/or device installations as well as for Cisco Unified Communications Manager nodes that have been upgraded from various releases.

**Note**

You do not need to obtain new licenses if you are upgrading within a software release train, such as Cisco Unified Communications Manager 6.0(1) to 6.1(1).
To obtain a license, see the section that applies to your situation:

- If you are installing new Cisco Unified Communications Manager servers or devices that require additional device license units, see the “Obtaining Licenses for New Cisco Unified Communications Manager Nodes and Devices” section on page 30-14.
- If you are upgrading from supported versions of Cisco Unified Communications Manager 6.x, see the “Obtaining a Software Feature License” section on page 30-15.

### Obtaining Licenses for New Cisco Unified Communications Manager Nodes and Devices

Use the following procedure to obtain a node license file for new Cisco Unified Communications Manager nodes (servers) and to obtain device licenses for new devices that require additional device license units.

Each node in your cluster requires one node license unit. Each device type requires a fixed number of licenses units, depending on the type. For example, Cisco Unified IP Phone 7920 requires four license units, and Cisco Unified IP Phone 7970 requires five units. If you want licenses for four Cisco Unified IP Phones 7920 and four Cisco Unified IP Phones 7970 phones, you require 36 phone license units.

Cisco Unified Communications Manager contains a starter licenses that you can use to begin new installations of Cisco Unified Communications Manager. The system overwrites the starter license when you obtain and upload your permanent licenses.

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary permanent licenses, as described in the following procedure.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager or phone order in the License Registration web tool at <a href="http://www.cisco.com/go/license">http://www.cisco.com/go/license</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Submit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must enter a valid e-mail address as well as the number of nodes and device license units for which you want licenses.</td>
</tr>
</tbody>
</table>

**Note**

For information on calculating the number of device license units that are required for the devices in your system, see the “Calculating the Number of Required License Units” section on page 30-12.

The system sends the license file(s) to you via e-mail by using the E-mail ID that you provided. The format of a license file specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

**Note**

One license file may apply to more than one node in your cluster. For information on how to interpret the license file, see the “Uploading a License File” section on page 30-16.

Step 4

You must upload the license file to the server with the matching MAC address that you provided in Step 3. See the “Uploading a License File” section on page 30-16. This server then takes on the functionality of the license manager.
You can use the licenses that are specified in the license file only within the cluster on which the license file is uploaded.

**Additional Information**
See the “Related Topics” section on page 30-22.

### Obtaining a Software Feature License

A software feature license activates features on your system for the specified license version. To use previous device license versions with this version of Cisco Unified Communications Manager, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.

Use this procedure to obtain a software feature license:

**Procedure**

**Step 1** Navigate to the License Registration web tool at [http://www.cisco.com/go/license](http://www.cisco.com/go/license).

**Step 2** Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager upgrade.

**Step 3** Click **Submit**.

**Step 4** Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must also enter a valid e-mail address.

The system sends the license file to you via e-mail by using the e-mail address that you provided. To view the contents of a software feature license, see the “Understanding the Contents of the License File” section on page 30-6.

**Step 5** You must upload the software license file to the server with the matching MAC address that you provided in **Step 4**. See the “Uploading a License File” section on page 30-16.

**Additional Information**
See the “Related Topics” section on page 30-22.

### Verifying That the License Manager Service Is Running

The Cisco Unified Communications Manager server where the license file is loaded assumes the functionality of a license manager. (The license file gets loaded on the first node only.) For information on license files, see the “Understanding How Licensing Works for Phones” section on page 30-8.

The license manager serves as the logical component that keeps track of the licenses that get purchased and used. It refers to the processes that control the checkin and checkout of the licenses. It keeps track of the number of license units that are required for each phone and application type. The license manager has responsibility for issuing and reclaiming licenses and for detecting whether an overdraft of licenses occurs.

Start the license manager service by using Cisco Unified Serviceability. This section describes the procedures to start, stop, or restart the service.
Working with Licenses

Note
Because license manager is a network service, it automatically starts and runs after the Cisco Unified Communications Manager installation.

Procedure

Step 1
In Cisco Unified Serviceability, choose Tools > Control Center - Network Services.
The Control Center–Network Services window displays.
Step 2
Choose the Cisco Unified Communications Manager server from the Servers drop-down list box.
Step 3
Click the radio button for Cisco License Manager.
Step 4
If you want to start the License Manager service, click Start.
Step 5
If you want to stop the License Manager service, click Stop.
Step 6
If you want to restart the License Manager, click Restart.

Additional Information
See the “Related Topics” section on page 30-22.

Uploading a License File

Use the following procedure to upload a license file to the Cisco Unified Communications Manager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the “Understanding How Licensing Works for Phones” section on page 30-8. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.

The License File Upload window may display a message that uploading the license file removes the starter (demo) licenses for the feature.

After you upgrade to Cisco Unified Communications Manager 8.5(1) from a compatible Cisco Unified CM 6.x release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated. Immediately after you complete the upgrade to Cisco Unified Communications Manager 8.5(1), upload the software feature license that is required for Cisco Unified Communications Manager 8.5(1) in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 8.5(1).

Note
Upload the license file only on the first node of Cisco Unified Communications Manager cluster.

Procedure

Step 1
Choose System > Licensing > License File Upload.
The License File Upload window displays.
Step 2  The Existing License Files drop-down list box displays the license files that are already uploaded to the server.

**Note**  To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.

Step 3  To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4  To upload to the server, click **Browse** to choose a license file.

**Note**  The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 5  Click **Upload**.

After the upload process completes, the Upload Result file displays.

Step 6  Click **Close**.

Step 7  In the License File Upload window, the status of the uploaded file displays. In Cisco Unified Serviceability, restart the Cisco CallManager service.

**Note**  The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

**Additional Information**

See the “Related Topics” section on page 30-22.

**Generating a License Unit Report**

Use the license unit report to display the total license capacity and the number of licenses in use. This tool generates a report that lists the total number of available licenses. The license unit report also displays the software license version that is installed on the Cisco Unified Communications Manager server.

**Note**  For more information on requesting licenses, see the “Obtaining a License File” section on page 30-13.

A unit license refers to a fixed number of device license units that correspond to each phone type. For example, Cisco Unified IP Wireless 7920 requires four device license units, and a Cisco Unified IP Phone 7970 requires five device license units. If you are provisioning four 7920 phones and four 7970 phones, you require 36 phone license units.
The number of licensed units in the license file corresponds to the number of unit licenses for all the
phone types that are purchased.

The License Unit Report window displays the status of a license file. For example, the Status column
for each license type may display Demo, Missing, Invalid, or Uploaded. If the status is Invalid, verify
that the license files have been obtained with a correct license MAC; that is, issue the `show status` cli
command from the command line interface to obtain the license MAC and compare that value to the
value that displays in the contents of the license file, which you view in the License File Upload window.
If the values do not match, obtain license files for the correct license MAC and upload in the License
File Upload window. For more information on cli commands, see the Command Line Interface Reference
Guide for Cisco Unified Communications Solutions.

**Note**

To determine the number of license unit that are required for each device, choose System > Licensing >
License Unit Calculator. This window lists the number of license units that are required for each type
of device.

Use the following procedure to generate a report for the number of licenses that are available.

**Procedure**

**Step 1** Choose System > Licensing > License Unit Report.

**Step 2** The License Unit Report window displays. This window displays the number of phone licenses, number
of node licenses, and software license versions. Phone and node licenses that are available display by
- Units Authorized
- Units Used
- Units Remaining

The software license version displays the
- License Server Name
- Cisco Unified Communications Manager Software Version

**Additional Information**

See the “Related Topics” section on page 30-22.

**License Capabilities Assignment Configuration Settings**

Capabilities Assignment allows system administrators to enable the Cisco Unified Presence (CUP) and
Cisco Unified Personal Communicator (CUPC) capabilities for users. You must ensure that licenses for
CUP and CUPC are available.

Make license capabilities assignments to existing users. Before you begin, ensure that users exist on your
system by choosing User Management > End User and clicking Find.

Before you begin configuring the capabilities assignments for users, determine how many CUP (servers
and clients) and CUPC licenses are required for your system by choosing Licensing > License Unit
Calculator. Acquire the required licenses by using Licensing > License File Upload. Verify the total
licenses by using Licensing > License Unit Report.
Table 30-5 describes the license capabilities assignment configuration settings. For related procedures, see the “Related Topics” section on page 30-22.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Information</strong></td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>Displays the name of the user for which you are enabling capabilities assignment.</td>
</tr>
<tr>
<td><strong>Capabilities Assignment Information</strong></td>
<td></td>
</tr>
<tr>
<td>Enable CUP (Cisco Unified Presence)</td>
<td>To enable CUP for this user, check the Enable CUP (Cisco Unified Presence) check box.</td>
</tr>
<tr>
<td>Enable CUPC (Cisco Unified Personal Communicator)</td>
<td>To enable CUPC for this user, check the Enable UPC (Cisco Unified Personal Communicator) check box. You can enable both CUP and CUPC; however, if you want CUPC, you must also enable CUP.</td>
</tr>
</tbody>
</table>

**Finding a License Capabilities Assignment**

Because you might have several license capabilities assignments for users in your network, Cisco Unified Communications Manager Administration lets you locate specific capabilities assignments on the basis of specific criteria. Use the following procedure to find locations.

**Note**  
During your work in a browser session, Cisco Unified Communications Manager Administration retains your location search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your location search preferences until you modify your search or close the browser.

**Procedure**

**Step 1** Choose **System > Licensing > Capabilities Assignment**.

The Find and List Capabilities Assignment window displays.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to **Step 3**.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

**Note**  
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criteria or click the **Clear Filter** button to remove all added search criteria.

**Step 3** Click **Find**.
All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

**Step 4**
From the list of records that display, click the link for the record that you want to view.

<table>
<thead>
<tr>
<th>Note</th>
<th>To reverse the sort order, click the up or down arrow, if available, in the list header.</th>
</tr>
</thead>
</table>

The window displays the item that you choose.

**Additional Information**
See the “Related Topics” section on page 30-22.

### Configuring the Capabilities Assignments for One User

This section describes how to add or update a capabilities assignment for a user to the Cisco Unified Communications Manager database.

**Before You Begin**
Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.

**Procedure**

**Step 1** Choose **System > Licensing > Capabilities Assignment**.
The Find and List Capabilities Assignment window displays.

**Step 2** To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the “Uploading a License File” section on page 30-16 and continue with **Step 3**.
The Capabilities Assignments Configuration window displays.

**Step 3** Check the appropriate check box as described in Table 30-5.

**Step 4** To save the capabilities assignment information in the database, click **Save**.

**Additional Information**
See the “Related Topics” section on page 30-22.

### Configuring the Capabilities Assignments for Multiple Users

This section describes how to add or update capabilities assignments for multiple users to the Cisco Unified Communications Manager database.

**Before You Begin**
Before configuring a capabilities assignment, you must obtain licenses from Cisco Systems by using the License File Upload under the System menu.
You can assign licenses for up to 250 users when you are using the bulk assignment capability.

Procedure

Step 1  Choose System > Licensing > Capabilities Assignment.

Step 2  To add a new capabilities assignment or update an existing capabilities assignment, locate the appropriate capabilities assignment as described in the “Uploading a License File” section on page 30-16 and continue with Step 3.

Step 3  To enable a new capabilities assignment or to update an existing capabilities assignment for multiple users, check the check boxes next to the users or click the Select All button.

Step 4  Click the Bulk Assignment button.

Step 5  Check the appropriate check box as described in Table 30-5.

Step 6  To save the capabilities assignment information in the database, click Save.

Troubleshooting Licensing

This section contains information on the following topics:

- Alarms, Alerts, and License Status Notification, page 30-21

Alarms, Alerts, and License Status Notification

Cisco Unified Communications Manager identifies the state of a license; that is, if it is missing, if it is a demo license, if it is an invalid license, or if it is an uploaded license. In addition, Cisco Unified Communications Manager Administration warns you whether Cisco Unified Communications Manager currently operates with starter licenses, with an insufficient number of licenses, or with an incorrect software feature license. For more information on this topic, see the “Understanding Licensing-Related Windows” section on page 30-4.

Tip

If the status is Invalid, verify that the license files have been obtained with a correct license MAC; that is, issue the show status cli command from the command line interface to obtain the license MAC and compare that value to the value that displays in the contents of the license file, which you view in the License File Upload window.

The following alarms get generated for licensing:

- CiscoLicenseManagerDown
Chapter 30      Licensing

Related Topics

- CiscoLicenseOverDraft
- CiscoLicenseRequestFailed
- CiscoLicenseDataStoreError
- CiscoLicenseInternalError
- CiscoLicenseFileError

Tip
To find these alarms, access the JavaApplications Alarm Catalog in Cisco Unified Serviceability. See the Cisco Unified Serviceability Administration Guide for more information on alarms.

If Cisco Unified Communications Manager does not have the appropriate license file, an alert gets generated; for information on alerts, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

For DNS, make sure that you map the IP addresses of all servers, including dummy nodes, to the hostnames on the DNS server. If you do not perform this task, Cisco Unified Communications Manager generates alarms that the License Manager service is down.

Additional Information
See the “Related Topics” section on page 30-22.

Related Topics

- Checklist for Licensing, page 30-2
- Understanding Licensing, page 30-3
  - Understanding Licensing Terminology, page 30-3
  - Understanding Licensing-Related Windows, page 30-4
  - Understanding the Contents of the License File, page 30-6
  - Understanding How Licensing Works for Phones, page 30-8
  - Understanding How Adjunct Licensing Works, page 30-9
  - Understanding How Licensing Works for Applications, page 30-9
- Interactions and Restrictions, page 30-11
- Working with Licenses, page 30-12
  - Calculating the Number of Required License Units, page 30-12
  - Obtaining a License File, page 30-13
  - Verifying That the License Manager Service Is Running, page 30-15
  - Uploading a License File, page 30-16
  - Generating a License Unit Report, page 30-17
  - License Capabilities Assignment Configuration Settings, page 30-18
  - Finding a License Capabilities Assignment, page 30-19
  - Configuring the Capabilities Assignments for One User, page 30-20
  - Configuring the Capabilities Assignments for Multiple Users, page 30-20
• Troubleshooting Licensing, page 30-21
• Licensing for Third-Party Phones That Are Running SIP, Cisco Unified Communications Manager Administration Guide
• Replacing a Single Server or Cluster for Cisco Unified Communications Manager
• Cisco Unified Serviceability Administration Guide
• Cisco Unified Real Time Monitoring Tool Administration Guide
• Command Line Interface Reference Guide for Cisco Unified Communications Solutions
Local Route Groups

This chapter provides the following information about local route groups:

- Configuration Checklist for Local Route Groups, page 31-1
- Introducing Local Route Groups, page 31-3
- Routing with Local Route Groups, page 31-5
- Simple Local Routing, page 31-6
- Tail End Hop Off, page 31-9
- Called Party Transformations, page 31-11
- System Requirements for Local Route Groups, page 31-13
- Interactions and Restrictions, page 31-13
- Installing and Activating Local Route Groups, page 31-15
- Configuring Local Route Groups, page 31-15
- Setting the Local Route Group Service Parameters, page 31-16
- Related Topics, page 31-16

Configuration Checklist for Local Route Groups

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).
Table 31-1 lists the tasks that you perform to configure the Local Route Group feature. For more information on the local route group feature, see the “Introducing Local Route Groups” section on page 31-3 and the “Related Topics” section on page 31-16.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| Step 1              | Review the interactions and restrictions for this feature. | Interactions, page 31-13  
|                     | Restrictions, page 31-15     |
| Step 2              | If you have not already done so, activate the Cisco CallManager service in Cisco Unified Serviceability. | Cisco Unified Serviceability Administration Guide |
| Step 3              | Use the Call Routing > Route/Hunt > Route List menu option in Cisco Unified Communications Manager Administration to configure a local route list that contains the Standard Local Route Group as a member of the route list. | Route List Configuration, Cisco Unified Communications Manager Administration Guide |
| Step 4              | Use the System > Device Pool menu option in Cisco Unified Communications Manager Administration to configure the Local Route Group setting for the device pools in the Cisco Unified Communications Manager implementation. For each device pool that you configure, specify a route group to use as local route group for that device pool. For each device pool, users may also configure the Called Party Transformation CSS for the devices in that device pool. | Device Pool Configuration, Cisco Unified Communications Manager Administration Guide |
|                     | If the dial plan is not globalized and the Local Route Group needs to use transformation patterns for called party, use the Device > Gateway and Device > Trunk menu options in Cisco Unified Communications Manager Administration to configure the gateways and trunks in each location. For each device that you want to configure for the Local Route Group feature, configure the following fields: | Gateway Configuration, Cisco Unified Communications Manager Administration Guide  
|                     | • Called Party Transformation CSS—Choose a CSS to allow localization of the called party number on the device. | Trunk Configuration, Cisco Unified Communications Manager Administration Guide  
|                     | • Use Device Pool Called Party Transformation CSS—Check this check box to use the Called Party Transformation CSS that is specified by the device pool to which this device belongs. If the check box is left unchecked, the Called Party Transformation CSS specified for the device gets used. |  |
| Step 6              | Use the Call Routing > Transformation Pattern > Called Party Transformation Pattern menu item in Cisco Unified Communications Manager Administration to configure the called party transformation pattern for the digits before a call is routed out through a gateway. | Called Party Transformation Pattern Configuration, Cisco Unified Communications Manager Administration Guide |
### Introducing Local Route Groups

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

Cisco Unified Communications Manager uses a special Local Route Group that can be bound to a provisioned route group differently based on the Local Route Group device pool setting of the originating device. Devices, such as phones, from different locales can therefore use identical route lists and route patterns, but Cisco Unified Communications Manager selects the correct gateway(s) for their local end.

### Note

This document uses the term *provisioned route group* to specify a route group that an administrator configures through use of the **Call Routing > Route/Hunt > Route Pattern** menu item in Cisco Unified Communications Manager Administration.

### Configuration Checklist for Local Route Groups (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Use the <strong>Call Routing &gt; Route/Hunt &gt; Route Pattern</strong> menu item in Cisco Unified Communications Manager Administration to configure the route patterns to use route lists that are configured to use the Standard Local Route Group.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Use the <strong>Call Routing &gt; Route Plan Report</strong> menu option in Cisco Unified Communications Manager Administration to generate and view the route plan report for your implementation. Check the route plan report to verify that the provisioning that you performed is correct for your Local Route Group configuration.</td>
</tr>
</tbody>
</table>

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).

In simple local routing cases, the provisioning gets reduced from N route patterns and N route lists to one route pattern and one route list. In cases with Tail End Hop Off (TEHO), local route groups allow configuration of N route patterns and N route lists instead of $N^2$ route patterns and $N^2$ route lists. Because values for N are now reaching much more than 1000 for larger implementations, enormous scalability savings result.

Previously, Cisco Unified Communications Manager treated gateways as devices to which multiple patterns are assigned. A tight, somewhat inflexible, binding existed between a gateway and the patterns that Cisco Unified Communications Manager associated with the gateway. When a call was placed, Cisco Unified Communications Manager viewed the situation as “Caller X has dialed some digits. These digits match pattern Y. Pattern Y directly associates with route lists, route groups, and gateways A, B, and C.”
The following subsections explain the details of provisioning local route groups and provide example scenarios:

- **Local Route Group**, page 31-4
- **Binding a Provisioned Route Group to a Local Route Group During a Call**, page 31-4
- **Routing with Local Route Groups**, page 31-5
- **Called Party Transformations**, page 31-11

**Additional Information**

See the “Related Topics” section on page 31-16.

### Local Route Group

When the administrator adds a new route group to a route list, the Route List Configuration window presents the administrator with all available route groups from which to select. This list includes as its first member the special route group that is named *Standard Local Route Group*. This local route group specifies a virtual local route group.

The local route group does not statically get bound to any provisioned route group. The local route group does not display in the Find and List Route Groups configuration window; and, therefore, cannot be deleted or modified. You can, however, add the local route group to any route list; when so added, the local route group serves as a placeholder for a provisioned route group that will later get bound to the local route group dynamically during call setup.

After you add the local route group to a route list, you can later remove it from that list, or you can modify its search-order places in the list as with any provisioned route group.

**Additional Information**

See the “Related Topics” section on page 31-16.

### Binding a Provisioned Route Group to a Local Route Group During a Call

Deferring the binding of a provisioned route group to the local route group until call setup ensures that the desired provisioned route group can be the one that is local to the device that is placing the call. Thus, a device in location X would use a provisioned route group that contains gateways for the location X PSTN while a device in location Y would use a different provisioned group of gateways for the location Y PSTN.

You need to ensure that each device in the system is provisioned to know its local route group. To avoid specifying this information in the configuration window for each device, because the number of devices can be many thousands, Cisco Unified Communications Manager Administration locates the information in the device pool for the device, because device pools specify common site-specific information.

The Local Route Group field in the Device Pool Configuration window includes a drop-down list box that lists all available (provisioned) route groups. This list excludes the special Standard Local Route Group name (because only provisioned route groups should be configured for a device pool) but presents the special name, `<NONE>`, which specifies the first (default) choice. Choose `<NONE>` if no binding is desired.
Whenever the default value <NONE> is selected for a device pool, any call that uses a route list that includes the local route group, Standard Local Route Group, gets routed as if the Standard Local Route Group is absent from the list.

With this mechanism, a call that is placed from any device over a route list that contains the special Standard Local Route Group behaves as follows:

1. The route list algorithm searches through the list of included route groups, in the designated order, until an unused trunk can be found. (The previous and current implementations do not differ.)

2. If the search encounters the special Standard Local Route Group, the system automatically replaces this route group with the name of the local route group that is provisioned for the calling device, unless the search encounters one of the following situations:
   - If the provisioned route group specifies <NONE>, the Standard Local Route Group route group gets skipped entirely.
   - If by skipping the Standard Local Route Group in this way, the search ends (that is, the Standard Local Route Group was the last or only route group in the route list), routing aborts, and the user receives reorder tone or an equivalent notification.

Additional Information
See the “Related Topics” section on page 31-16.

Routing with Local Route Groups

With local route group mapping, Cisco Unified Communications Manager can treat gateways more like a service. Customers benefit by reducing the efforts of provisioning and maintaining the routes plans from this solution.

Example
This example assumes a centralized call model with five managed sites as shown in Figure 31-1. Further sections use this call model to demonstrate the two different manifestations of the Local Route Groups feature as follows:

- Simple local routing cases in which each site needs to route offnet calls to its local gateways
- More complex tail end hop off (TEHO) cases
Introducing Local Route Groups

A Cisco Unified Communications Manager deployment that uses the Local Route Group feature must normalize the called digits through Called Party Transformation to guarantee that an intended destination can be reached.

Additional Information
See the “Related Topics” section on page 31-16.

Simple Local Routing

Simple local routing comprises cases in which each site needs to route offnet calls to its local gateways. Provisioning of route patterns and route lists can get reduced from the need to configure N route patterns and N route lists to a configuration where only one route pattern and one route list are needed.

For this case further assume that all phones that home to a particular site belong to a single calling search space (CSS) that is unique to that site. For example, phones at the Boulder site belong to the CSS-Bldr calling search space and so forth. Figure 31-2 illustrates a possible provisioning of this system without using the Local Route Group feature, so regardless of site, a phone always prefers its local gateway when making an offnet call by dialing 9 followed by a seven-, ten-, or eleven-digit pattern. As more sites get added, each of the columns must include new entries (rows). If N sites exist, you need N different route lists, route patterns, partitions, and calling search spaces.
### Figure 31-2  Provisioning Local Offnet Access Without Local Route Groups

<table>
<thead>
<tr>
<th>Sites</th>
<th>Gateway Devices</th>
<th>Route Groups</th>
<th>Device Pools</th>
<th>Route Lists</th>
<th>Partitions</th>
<th>Route Patterns</th>
<th>Calling Search Spaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boulder, CO</td>
<td>GW-Bldr</td>
<td>RG-Bldr</td>
<td>DP-Bldr</td>
<td>RL-Bldr</td>
<td>P-Bldr</td>
<td>9.@/P-Bldr</td>
<td>CSS-Bldr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GW:GW-Bldr</td>
<td></td>
<td>RG:RG-Bldr</td>
<td></td>
<td>RL:RL-Bldr</td>
<td></td>
</tr>
<tr>
<td>Herndon, VA</td>
<td>GW-Hrdn</td>
<td>RG-Hrdn</td>
<td>DP-Hrdn</td>
<td>RL-Hrdn</td>
<td>P-Hrdn</td>
<td>9.@/P-Hrdn</td>
<td>CSS-Hrdn</td>
</tr>
<tr>
<td>Richardson, TX</td>
<td>GW-Rch</td>
<td>RG-Rch</td>
<td>DP-Rch</td>
<td>RL-Rch</td>
<td>P-Rch</td>
<td>9.@/P-Rch</td>
<td>CSS-Rch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GW:GW-Rch</td>
<td></td>
<td>RG:RG-Rch</td>
<td></td>
<td>RL:RL-Rch</td>
<td></td>
</tr>
<tr>
<td>RTP, NC</td>
<td>GW-RTP</td>
<td>RG-RTP</td>
<td>DP-RTP</td>
<td>RL-RTP</td>
<td>P-RTP</td>
<td>9.@/P-RTP</td>
<td>CSS-RTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GW:GW-RTP</td>
<td></td>
<td>RG:RG-RTP</td>
<td></td>
<td>RL:RL-RTP</td>
<td></td>
</tr>
<tr>
<td>San Jose, CA</td>
<td>GW-SJ</td>
<td>RG-SJ</td>
<td>DP-SJ</td>
<td>RL-SJ</td>
<td>P-SJ</td>
<td>9.@/P-SJ</td>
<td>CSS-SJ</td>
</tr>
</tbody>
</table>
Introducing Local Route Groups

In the same implementation, use of the Local Route Group feature allows configuration of a single route list, partition, route pattern, and CSS, regardless of the number of sites, as shown in Figure 31-3.

**Figure 31-3 Provisioning Local Offset Access With Local Route Groups**

<table>
<thead>
<tr>
<th>Sites</th>
<th>Gateway Devices</th>
<th>Route Groups</th>
<th>Device Pools</th>
<th>Route Lists</th>
<th>Partitions</th>
<th>Route Patterns</th>
<th>Calling Search Spaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boulder, CO</td>
<td>GW-Bldr</td>
<td>RG-Bldr</td>
<td>DP-Bldr</td>
<td>RL-Local</td>
<td>P-System</td>
<td>9.@/P-System</td>
<td>CSS-System</td>
</tr>
<tr>
<td>Herndon, VA</td>
<td>GW-Hrdn</td>
<td>RG-Hrdn</td>
<td>DP-Hrdn</td>
<td></td>
<td>P-System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richardson, TX</td>
<td>GW-Rch</td>
<td>RG-Rch</td>
<td>DP-Rch</td>
<td>RL:RL-Local</td>
<td>P-System</td>
<td>9.@/P-System</td>
<td>CSS-System</td>
</tr>
<tr>
<td>RTP, NC</td>
<td>GW-RTP</td>
<td>RG-RTP</td>
<td>DP-RTP</td>
<td></td>
<td>P-System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Jose, CA</td>
<td>GW-SJ</td>
<td>RG-SJ</td>
<td>DP-SJ</td>
<td></td>
<td>P-System</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this case, the following configuration applies:

- All phones belong to a single CSS-System calling search space and to a single P-System partition.
- All phones for a given site belong to a single device pool unique to that site.
- The Local Route Group field in each device pool identifies the specific route group for that site. In this example, RG-Bldr for Boulder, RG-Rch for Richardson, and so on.

Thus, the route lists, route patterns, partitions and calling search spaces for this case each get reduced from N to 1. The number of gateways, route groups, and device pools remain N for N sites.

A new partition, P_System, and a new calling search space, CSS_System, get added for accessing the 9.@ pattern from all sites. The calling search space, CSS_Boulder, can contain both P_Boulder and P_System as well, as can the CSS of the other sites.

**Additional Information**

See the “Related Topics” section on page 31-16.
Tail End Hop Off

Tail End Hop Off (TEHO) refers to routing long-distance calls across the VoIP network and dropping them off to the Public Switched Telephone Network (PSTN), as a local call, at a remote gateway. In TEHO situations, you can reduce the configuration complexity from the need to configure $N^2$ entities to needing only $N$ entities. The following assumptions for TEHO apply:

- Each site has a different route pattern and route list for each of the other $N-1$ sites.
- For a given site, $S$, each of the $N-1$ route lists to another (remote) site has, as first preference, a route group of one or more gateways that are local to that other site followed by, as second preference, a route group that is local to $S$. Therefore, when sufficient trunking resources are available to honor the first preference, a long-distance call uses a gateway at the remote site to go offnet and thus bypass any tolls; otherwise, the call defaults to a local gateway and incurs toll charges.

Again, Cisco Unified Communications Manager has an identical routing policy for all sites. The second preference of routing a call through the local PSTN of a site (if the system fails to drop off the call as a local call at the remote PSTN) forces the customer to provision separate instances of all routing information for each site, as illustrated in Figure 31-4. (The figure illustrates the configuration for some of the sites.) Each site has a unique set of route patterns and route lists to each of the other $N-1$ sites, as well as a generic local route list for all other calls that the remote access codes do not cover. This requirement entails a total of $N \times (N-1) + N$, or $N^2$, route lists and route patterns for the general case.
Using the Local Route Group feature, the $N \times (N-1)$ route patterns and route lists that are needed for remote sites reduce to $N$, and the $N$ local route patterns and local route lists reduce to 1. Overall, the total number of route lists and route patterns decreases from $N^2$ to $N+1$, and calling search spaces and partitions decrease from $N$ to 1, as illustrated in Figure 31-5.
In Figure 31-5, note the crucial element, which is the use of the Standard Local Route Group as the second choice in each route list. The setting in the device pool of the originating device dynamically determines the actual provisioned route group that gets used during a specific call.

**Additional Information**

See the “Related Topics” section on page 31-16.

### Called Party Transformations

While loose coupling occurs between the enterprise number and the route group/gateway, very tight coupling occurs between the route group/gateway and the patterns that the PSTN expects. If the gateway chosen is in a 7-digit dialing location, the PSTN expects 7 digits; if the chosen gateway is in a 10-digit location, the PSTN expects 10 digits to access local numbers.

**Example 1**

A call gets placed from Dallas; the called number specifies 9.5551212. If the Dallas local gateway is busy or not accessible, assuming that the San Jose gateway is selected, 9.5551212 must be converted to 1 214 555 1212 for the San Jose gateway to dial out.

In the same example for a Local Route Group case, a call gets placed from Dallas. The called number specifies 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed by the originator, discard PreDot, and insert the prefix +1 214.
2. Convert the call number to a globally unique E.164 string (+1 214 555 1212).

If a San Jose gateway gets selected, the system converts the global string +1 214 555 1212 to 1 214 555 1212; if a Dallas gateway gets selected, the system converts the global string to 214 555 1212.
See Figure 31-6 for an illustration of this example.

**Figure 31-6  Called Digits Transformation**

---

**Example 2**

A call gets placed from RTP; the called number specifies 5551212. If the RTP local gateway is busy or not accessible, assuming that the San Jose gateway is selected, 5551212 must get converted to 1 919 555 1212 for the San Jose gateway to dial out.

In the same example for a Local Route Group case, a call gets placed from RTP. The called number specifies 9.5551212, so the system must perform the following actions:

1. Take the digits as dialed, discard PreDot, and insert the Prefix 91919.
2. Convert the called number to a global dialing string (91 919 555 1212).

If a San Jose gateway gets selected, the system converts the global string 91 919 555 1212 to 1 919 555 1212; if the RTP gateway gets selected, the system converts the global string to 555 1212.

**Additional Information**

For more details about called party transformations, see the “Called Party Number Transformations Settings” section in the “Understanding Route Plans” of the *Cisco Unified Communications Manager System Guide*.

For details about the international + escape character, see the “Using the International Escape Character +” section in the “Understanding Route Plans” of the *Cisco Unified Communications Manager System Guide*.

Also, see the “Related Topics” section on page 31-16.
System Requirements for Local Route Groups

The following system requirement applies to the local route group feature:

- Cisco Unified Communications Manager 7.0(1) or later

Additional Information
See the “Related Topics” section on page 31-16.

Interactions and Restrictions

The following sections describe the interactions and restrictions for local route groups:

- Interactions, page 31-13
- Restrictions, page 31-15

Additional Information
See the “Related Topics” section on page 31-16.

Interactions

The following sections describe how the local route group feature interacts with other Cisco Unified Communications Manager features and applications:

- Supported Devices, page 31-13
- Forwarding, page 31-14
- Other Supplementary Services, page 31-14
- Route Plan Report, page 31-14
- Cisco Unified Mobility, page 31-15

Additional Information
See the “Related Topics” section on page 31-16.

Supported Devices

All Cisco Unified Communications Manager device types that are capable of originating a call support support the Local Route Group feature, including the following devices:

- Skinny devices
- H.323 devices
- SIP devices
- MGCP devices, including all PRI variants, BRI, and MGCP phones
- CTI devices
Forwarding

For forwarded calls, Cisco Unified Communications Manager must use the Local Route Group that is provisioned in the device pool settings that are associated with the redirected party to find the provisioned local route group. Thus, if phone A calls (local) phone B and phone B forwards the call to (remote) phone C, the Local Route Group value from the phone A device pool gets used rather than the corresponding value for phone B.

Other Supplementary Services

Many supplementary services can originate calls. When this happens, the local route group gets skipped. The following features can initiate calls:

- CallBack
- MWI
- Mobility (FollowMe)
- Path Replacement

If by skipping the Standard Local Route Group route group, the search ends (that is, the Standard Local Route Group represents the last or only route group in the route list), routing aborts.

The following features can redirect calls:

- Barge
- CallBack
- Call Park
- Conference
- Directed Call Park
- Forwarding
- Immediate Divert
- MeetMe Conference
- Call Pickup

As explained in the “Forwarding” section on page 31-14, Cisco Unified Communications Manager uses the Local Route Group that is provisioned in the device pool settings that are associated with the redirected party to find the provisioned local route group.

Route Plan Report

The Route Plan Report displays the route details, such as route list, associated route groups, and trunks/gateways, including the special Standard Local Route Group route group. An example follows.

Example of Route Plan Report Display for Route Patterns With No Local Route Group

```
BoulderRouteList
 |__ BoulderRG
    __BoulderGW1
       |__BoulderGW2
```
Cisco Unified Mobility

For Single Number Reach calls to a remote destination, the device pool of the originating calling party determines the selection of the Standard Local Route Group.

Restrictions

Before you configure local route groups, review the following restriction:

- Mixed Route Lists, page 31-15

Mixed Route Lists

You cannot insert SIP route groups and Q.SIG route groups into a route list at the same time. With the Local Route Group feature, this mixed route list rule cannot get enforced during provisioning because the binding between the Standard Local Route Group and a provisioned route group occurs dynamically during the call setup. Therefore, some Q.SIG related features may not be available. The binding from Standard Local Route Group to a Q.SIG route group should be avoided.

Additional Information

See the “Related Topics” section on page 31-16.

Installing and Activating Local Route Groups

After you install Cisco Unified Communications Manager, Release 7.0(1) or later, you can configure local route groups.

Additional Information

See the “Related Topics” section on page 31-16.

Configuring Local Route Groups

This section contains information on the following topics:

- Setting the Local Route Group Service Parameters, page 31-16

Tip

Before you configure local route groups, review the “Configuration Checklist for Local Route Groups” section on page 31-1.

Additional Information

See the “Related Topics” section on page 31-16.
Setting the Local Route Group Service Parameters

The Local Route Group feature does not require the configuration of any additional service parameters.

Additional Information
See the “Related Topics” section on page 31-16.

Related Topics

- Configuration Checklist for Local Route Groups, page 31-1
- Introducing Local Route Groups, page 31-3
- Local Route Group, page 31-4
- Binding a Provisioned Route Group to a Local Route Group During a Call, page 31-4
- Routing with Local Route Groups, page 31-5
- Called Party Transformations, page 31-11
- System Requirements for Local Route Groups, page 31-13
- Interactions and Restrictions, page 31-13
- Installing and Activating Local Route Groups, page 31-15
- Configuring Local Route Groups, page 31-15
- Setting the Local Route Group Service Parameters, page 31-16
- Route List Configuration, Cisco Unified Communications Manager Administration Guide
- Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Trunk Configuration, Cisco Unified Communications Manager Administration Guide
- Called Party Transformation Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Calling Party Transformation Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Route Plan Report, Cisco Unified Communications Manager Administration Guide
- Route Group Configuration, Cisco Unified Communications Manager Administration Guide
- Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide
- Partition Configuration, Cisco Unified Communications Manager Administration Guide
- Understanding Cisco Unified Communications Manager Voice Gateways, Cisco Unified Communications Manager System Guide
- Understanding Route Plans, Cisco Unified Communications Manager System Guide
- Partitions and Calling Search Spaces, Cisco Unified Communications Manager System Guide
- System-Level Configuration Settings, Cisco Unified Communications Manager System Guide
Logical Partitioning

The Logical Partitioning feature specifies the capability of a telephony system to control calls and features on the basis of specific allowed or forbidden configurations. A common telephony system can provide access to Voice over Internet Protocol (VoIP) and Public Switched Telephone Networks (PSTN), and configuration can control access.

This chapter contains information on the following topics:

- Configuration Checklist for Logical Partitioning, page 32-1
- Introducing Logical Partitioning, page 32-4
- Overview of Logical Partitioning Architecture, page 32-8
- Enterprise Parameters for Logical Partitioning, page 32-10
- System Requirements for Logical Partitioning, page 32-22
- Interactions and Limitations, page 32-22
- Configuring Logical Partitioning, page 32-39
- Logical Partitioning Configuration Upon Upgrade From Previous Releases, page 32-47
- Troubleshooting Logical Partitioning, page 32-47
- Related Topics, page 32-47

Configuration Checklist for Logical Partitioning

Logical partitioning allows configuration of Cisco Unified Communications Manager systems, so single-line phones, multiline phones, and analog phones can get configured to prevent restricted calls that mix VoIP and PSTN resources when calls occur between different geolocations. Only geolocations (in the Phone Configuration window) and geolocation filters (in the Device Pool Configuration window) can get configured for phones.
Table 32-1 provides a checklist for configuring logical partitioning. For more information on logical partitioning, see the “Related Topics” section on page 32-47.

### Table 32-1  Logical Partitioning Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable logical partitioning by setting the value of the Enable Logical Partitioning enterprise parameter to <em>True</em>.</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Define a set of geolocations on a new Geolocation Configuration window.</td>
</tr>
<tr>
<td></td>
<td>Geolocation Configuration, page 24-10</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.</td>
</tr>
<tr>
<td></td>
<td>Device Pool Configuration Settings, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Gateway Configuration Settings, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Displaying the MAC Address of a Phone, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Trunk Configuration Settings, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.</td>
</tr>
<tr>
<td></td>
<td>Geolocation Configuration, page 24-10</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Define the Logical Partitioning Default Policy, which determines whether to allow or deny PSTN calls between devices that associate with valid geolocations and geolocation filters when no explicit Allow/Deny policy is configured in the Logical Partitioning Policy Configuration window for the related geolocation policy records.</td>
</tr>
<tr>
<td></td>
<td>Use the Enterprise Parameters Configuration window to set the value for the Logical Partitioning Default Policy enterprise parameter.</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, <em>Cisco Unified Communications Manager Administration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
</tbody>
</table>
Table 32-1  Logical Partitioning Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> For devices that do not participate in logical partitioning policy checks, define the geolocation as <em>Unspecified</em> or leave undefined.</td>
<td>Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide Gateway Configuration Settings, Cisco Unified Communications Manager Administration Guide Displaying the MAC Address of a Phone, Cisco Unified Communications Manager Administration Guide Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
<tr>
<td><strong>Step 7</strong> Define a set of filter rules in a new Geolocation Filter Configuration window.</td>
<td>Geolocation Filter Configuration, page 24-17</td>
</tr>
<tr>
<td><strong>Step 8</strong> Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.</td>
<td>Device Pool Configuration Settings, Cisco Unified Communications Manager Administration Guide Gateway Configuration Settings, Cisco Unified Communications Manager Administration Guide Trunk Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 9</strong> Assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.</td>
<td>Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide Enterprise Parameters for Logical Partitioning, page 32-10</td>
</tr>
<tr>
<td><strong>Step 10</strong> Define a set of logical partitioning policy records in a new Logical Partitioning Policy Configuration window.</td>
<td>Logical Partitioning Policy Configuration, page 32-40</td>
</tr>
</tbody>
</table>
Introducing Logical Partitioning

Logical partitioning specifies a call control feature in Cisco Unified Communications Manager that provides functionality, so communication between the following pairs of VoIP entities can be controlled:

1. A VoIP phone and a VoIP gateway
2. A VoIP gateway and another VoIP gateway
3. An intercluster trunk and a VoIP phone
4. An intercluster trunk and a VoIP gateway

Options exist to configure Cisco Unified Communications Manager, so any such set of VoIP devices may be allowed communication with each other and any device can be restricted to one device or to a group of devices. No logical partitioning policy logic exists on endpoints.

Be aware that logical partitioning is required to control such communication not only during basic call establishment but also during mid-call as a result of midcall features.

The Cisco Unified Communications Manager basic routing policy constructs of calling search spaces and partitions suffice to prevent forbidden basic calls from being established but are not sufficient to prevent forbidden calls from being created as a result of midcall features. In Cisco Unified Communications Manager, such midcall features are often termed Join and Redirect features, because these primitives often get used internally to affect these features.

Logical partitioning enhances Cisco Unified Communications Manager to handle such midcall scenarios. Configuration for logical partitioning remains independent of supplementary features, where the policy checking gets performed based on devices being joined or redirected to a supplementary feature.

Note

Logical partitioning policy checks get performed later than digit analysis/calling search space/partition logic during call processing.
The logical partitioning solution comprises the following elements:

- **Identifiers**—A framework to associate a unique identifier with every device.
- **Policies**—Allow administrator the ability to define rules or policies that determine the interconnection between any two devices (a VoIP phone and a gateway) in the Cisco Unified Communications Manager system. The configured policies work bidirectionally between the pair of devices.
- **Policy Checking**—Call processing and features such as transfer, pickup, and ad hoc conference check the defined policies before allowing the calls or features between participants.

**Identifiers**

Identifiers specify a device type for every device (element) in a Cisco Unified Communications Manager logical partitioning solution. Device types classify all elements into two types: interior and border. **Table 32-2** specifies the Cisco Unified Communications Manager devices that associate with each device type:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Cisco Unified Communications Manager Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border</td>
<td>Gateway (for example, H.323 Gateway)</td>
</tr>
<tr>
<td></td>
<td>Intercluster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlled</td>
</tr>
<tr>
<td></td>
<td>H.225 trunk</td>
</tr>
<tr>
<td></td>
<td>SIP trunk</td>
</tr>
<tr>
<td></td>
<td>MGCP port (E1, T1, PRI, BRI, FXO)</td>
</tr>
<tr>
<td>Interior</td>
<td>Phones (SCCP, SIP, third party)</td>
</tr>
<tr>
<td></td>
<td>CTI route points</td>
</tr>
<tr>
<td></td>
<td>VG224 analog phones</td>
</tr>
<tr>
<td></td>
<td>MGCP port (FXS)</td>
</tr>
<tr>
<td></td>
<td>Cisco Unity Voice Mail (SCCP)</td>
</tr>
</tbody>
</table>

**Note**

You cannot edit the classification of Cisco Unified Communications Manager elements: only border and interior designations are allowed, and a particular device can be classified only according to the scheme that **Table 32-2** provides. For example, a SIP trunk can be classified only as a border element.

See the “Geolocation Identifiers” section on page 24-8 for further information. See “Geolocation Examples” section on page 24-8 for examples of geolocation identifiers.
Introducing Logical Partitioning

Allow and Deny Policies

Based on the system requirements for VoIP network topology, you can configure Cisco Unified Communications Manager to provide the following default system policy for logical partitioning:

- **Deny**—Calls or features get blocked between VoIP device participants of types 1 to 4 (previously enumerated).
  
  To allow VoIP communication, ensure the Allow policy is configured through logical partitioning configuration.

- **Allow**—Be aware that calls or features are allowed between VoIP device participants of types 1 to 4 (previously enumerated).
  
  To deny VoIP communication, ensure the Deny policy is configured through logical partitioning configuration.

Additional Information

See the “Related Topics” section on page 32-47.

Applicability to Requirements From Indian Telecom Regulations

Regulations of the Telecom Regulatory Authority of India (TRAI) require that voice traffic over the enterprise data network and the Public Switched Telephone Network (PSTN) must be strictly separated and no mixing of calls between the two networks can occur for the purpose of toll bypass.

The following list shows basic scenarios that are restricted (that is, not allowed):

- The call that passes through a PSTN gateway connects directly by using WAN to a VoIP phone or VoIP PSTN gateway in a different geographic location.
  
  - If PSTN gateway is located in India, this remains strictly restricted. If the PSTN is in another country and a VoIP phone is in India and if connection results in revenue loss to Indian telecom service providers, the connection gets considered restricted.

The following list gives basic scenarios that are permitted:

- Call directly between two VoIP phones in different geographic locations
- Call from a VoIP phone to a PSTN gateway in the same geographic location

A call that passes through a PSTN gateway must never connect directly to a VoIP phone or VoIP PSTN gateway in a different site or geographic location (geolocation) through use of IP telephony.

Requirement for Deployments

While following TRAI regulations and avoiding toll bypass, a single-line phone should be able to reach outside VoIP (closed user group [CUG]) or PSTN networks, provided that the suggested configuration guidelines are met.

**Note**

Ensure logical partitioning is enabled to avoid any toll bypass.
Available Cisco Unified Communications Manager Support
Cisco Unified Communications Manager prior to implementation of the logical partitioning feature provides the following support:

- Phones can use the same line to reach the VoIP or PSTN networks.
- The existing calling search space (CSS) and partitions mechanism allows partitioning of the network for basic calls only.

Limitations With a Single Line
The following limitations exist when a single line is used without (or prior to) configuration of the logical partitioning feature:

- Possible midcall Join—A call that connects to a VoIP network on WAN and another call that is made to a PSTN network may get joined upon invocation of a supplementary feature such as Transfer.
- Possible redirects—A call that comes from a VoIP network on WAN may get redirected to a PSTN network upon invocation of a supplementary feature such as Forwarding.

Without the logical partitioning feature, you cannot configure supplementary features to prevent invocation of the restricted scenarios.

Existing Deployments Prior to Use of Logical Partitioning
In India and other countries, separate lines on phones get used to separate the VoIP (CUG) and PSTN networks. This implementation previously prevented use of low-cost analog phones and single-line VoIP phones.

In deployments that use two-line phones, invocation of supplementary features like Join Across Lines (JAL) or Direct Transfer Across Line (DTAL) can result in scenarios that are restricted by TRAI regulations. For such deployments to conform to the regulations, you need the logical partitioning feature.

Additional Information
See the “Related Topics” section on page 32-47.

History
Originally, Indian regulations required that Voice over IP (VoIP) systems be physically separate from PSTN interconnect systems. Users used phones on a VoIP system strictly for interoffice phone calls, but any calls that needed to go to or come from the PSTN had to be made by using the PSTN system. Telecom Regulatory Authority of India (TRAI) regulations as of 2008 permit a single system to support both types of calls, as long as the system can be configured so that forbidden calls cannot complete. In a Cisco Unified Communications Manager system, the term logical partitioning specifies this capability.

The Enterprise VoIP implementations that use releases of Cisco Unified Communications Manager prior to Release 7.1(x) in India use the same Cisco Unified IP Phone for both the VoIP and PSTN connectivity. Cisco Unified Communications Manager does not support specific configurations for controlling the mixing of VoIP and PSTN traffic when supplementary features are invoked from a single line with participants in VoIP or PSTN domains. To comply with regulations, previous VoIP implementations in India used separate lines on VoIP phones for PSTN and VoIP calls.

Cisco Unified Communications Manager uses the concept of partitions and calling search spaces (CSS) for configuration of the respective lines. Thus, control remains separate for the VoIP and PSTN domains, and features like Transfer cannot be performed on single-line phones, because invoking such features could result in joining the VoIP with the PSTN network.
With this limitation, enterprise VoIP deployments in India that use Cisco equipment remained limited to using phones with minimum of two lines, which is not a cost-effective solution for most customers. This limitation also prevented solutions that use low-cost analog phones that are single line by design and use VG224/VG248 gateways.

To overcome the limitations, a Cisco Unified Communications Manager solution now allows logical partitioning of a single line on Cisco Unified IP Phones through administrator policies. Be aware that control of call joining or call redirection is required, based on an attribute tag or the geolocation of the parties.

Additional Information
See the “Related Topics” section on page 32-47.

Overview of Logical Partitioning Architecture

The logical partitioning solution entails provisioning the following elements:

- Configure geolocation identifiers
  - Administrator can define sets of geolocations (civic addresses).
  - Administrator can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
  - Administrator can define filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.

- Configure policies
  - Allow administrator to define geolocation policy records and define matrices of geolocation policy records that contain a policy that indicates whether a connection is permitted or denied. The configured policies work bidirectionally between the pair of devices.

- Communicate geolocation information across clusters
  - Allow communication of geolocation information from one cluster to another, both at call establishment as well as midcall joins and redirects.

Additional Information
See the “Related Topics” section on page 32-47.

Logical Partitioning Use of Geolocations and Geolocation Filters

Cisco Unified Communications Manager administrators must define the following items:

- A geolocation for every device that uses logical partitioning. See the “Geolocation Characteristics” section on page 24-6 for details.

- A geolocation filter for every device that uses logical partitioning. See the “Introducing Geolocation Filters” section on page 24-16 for details.

Cisco Unified Communications Manager administrators then assign geolocations and geolocation filters to devices.
The following entities in a Cisco Unified Communications Manager cluster can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports

Note: Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

Media devices, such as media termination points (MTP), conference bridges (CFB), announciators, and music on hold (MOH) servers, do not need to be associated with geolocations and geolocation filters.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device-pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The call processing and feature layer uses this information for logical partitioning policy checking.

The standard record for a geolocation specifies Unspecified. Use this value when no geolocation needs to associate with a device. For a device, if the geolocation specifies Unspecified or the geolocation filter specifies None, no identifier gets created, and the device does not participate in logical partitioning policy checks.

Be aware that the Default Geolocation enterprise parameter and the Logical Partitioning Default Filter enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Examples of Geolocations and Geolocation Filters

See Table 24-4 in the “Geolocations and Location Conveyance” chapter for examples of geolocations.

See Table 24-6 in the “Geolocations and Location Conveyance” chapter for examples of geolocation filters.

Additional Information

See the “Related Topics” section on page 32-47.
Logical Partitioning Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, the actual connected device is not known until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- The logical partitioning policy checks in the feature layer or LPSession process get ignored until the device answers and the actual geolocation information for the device becomes available.
- This behavior impacts the Early attended Transfer and Early attended Conference features by delaying the logical partitioning policy check until answer time.

Additional Information
See the “Related Topics” section on page 32-47.

Logical Partitioning Usage of Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

See the “Geolocation Identifiers” section on page 24-8 of the “Geolocations and Location Conveyance” for details.

Additional Information
See the “Related Topics” section on page 32-47.

Enterprise Parameters for Logical Partitioning

You can use the following enterprise parameters to configure logical partitioning:

- Enable Logical Partitioning—This parameter determines whether the logical partitioning feature is enabled. Logical partitioning policies get used for restricting calls and other supplementary features such as transfer, forward, conferences including Meet-Me, and so on. Valid values specify True (enable logical partitioning) or False (do not enable logical partitioning). When this parameter is set to False, calls do not get validated against any logical partitioning policy. This represents a required field. The default value specifies False.

- Default Geolocation—This parameter determines the default geolocation setting for all devices and device pools that do not have a specified geolocation in Cisco Unified Communications Manager Administration. Valid values include the names of all the geolocations that have been configured in the Geolocation Configuration window in Cisco Unified Communications Manager Administration. The default geolocation can get overridden on a per-device and per-device-pool basis in the Device Configuration window or the Device Pool Configuration window in Cisco Unified Communications Manager Administration. This represents a required field. The default value specifies Unspecified.

- Logical Partitioning Default Policy—This parameter determines the default policy for allowing or denying calls between geolocations. Before calls between geolocations are allowed to proceed, Cisco Unified Communications Manager checks to be sure that calls are allowed between the specified geolocations based on the setting in the Logical Partitioning Policy Configuration window in Cisco Unified Communications Manager Administration. If Use System Default is specified in
the Logical Partitioning Policy Configuration window, the value in this parameter determines whether calls are allowed or denied. Valid values specify Allow (allow calls to proceed) or Deny (do not allow calls to proceed). This represents a required field. The default value specifies Deny.

- Logical Partitioning Default Filter—This parameter determines the default filter for geolocations in the logical partitioning feature. Applying a filter to geolocations allows you to reduce the number of fields on the Geolocation Configuration window that apply to devices and device pools that belong to that geolocation. To choose a filter in this parameter, you must ensure that the filter is already configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. Valid values include None (do not include any geolocation fields) and the names of all the filters that are configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. The default value specifies None.

Additional Information
See the “Related Topics” section on page 32-47.

Logical Partitioning Policies

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

Ensure Allow and Deny policies are configured. See the “Allow and Deny Policies” section on page 32-6 for configuration details.

In the Logical Partitioning Policy Configuration window (Call Routing > Logical Partitioning Policy Configuration menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations. See the “Logical Partitioning Policy Configuration” section on page 32-40 for details of using Cisco Unified Communications Manager Administration to create logical partitioning policy records.

Configure logical partitioning policies between pairs of geolocation policy records and device types.

Example of Logical Partitioning Policy

({geolocpolicy1, devType1}, {geolocpolicy2, devType2}, Allow)

The following tables show the construction of a logical partitioning policy among geolocations, device types, and policy types.

First, assume the following geolocation policy records:

<table>
<thead>
<tr>
<th>Geolocation Policy</th>
<th>Record Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLRBLD1GeolocPolicy</td>
<td>(country=IN, A1=KA, A3=Bangalore, LOC=BLD1)</td>
</tr>
<tr>
<td>BLRBLD2GeolocPolicy</td>
<td>(country=IN, A1=KA, A3=Bangalore, LOC=BLD2)</td>
</tr>
</tbody>
</table>

The following tables show the construction of a logical partitioning policy among geolocations, device types, and policy types.
Enterprise Parameters for Logical Partitioning

Chapter 32  Logical Partitioning

From these records, you can configure the following sample logical partitioning policies. The system default policy specifies DENY.

<table>
<thead>
<tr>
<th>Geolocation Policy</th>
<th>Record Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUMBLD1GeolocPolicy</td>
<td>(country=IN, A1=MH, A3=Mumbai, LOC=BLD1)</td>
</tr>
<tr>
<td>blankGeolocPolicy</td>
<td>() – All fields blank</td>
</tr>
</tbody>
</table>

The first logical partitioning policy,

<table>
<thead>
<tr>
<th>Source</th>
<th>Geolocation Policy1</th>
<th>Target</th>
<th>Geolocation Policy2</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border</td>
<td>BLRBLD1GeolocPolicy</td>
<td>Interior</td>
<td>BLRBLD1GeolocPolicy</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Border</td>
<td>BLRBLD1GeolocPolicy</td>
<td>Border</td>
<td>BLRBLD1GeolocPolicy</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Border</td>
<td>BLRBLD2GeolocPolicy</td>
<td>Interior</td>
<td>BLRBLD2GeolocPolicy</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Border</td>
<td>BLRBLD2GeolocPolicy</td>
<td>Border</td>
<td>BLRBLD2GeolocPolicy</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Border</td>
<td>MUMBLD1GeolocPolicy</td>
<td>Interior</td>
<td>MUMBLD1GeolocPolicy</td>
<td>ALLOW</td>
</tr>
<tr>
<td>Border</td>
<td>MUMBLD1GeolocPolicy</td>
<td>Border</td>
<td>MUMBLD1GeolocPolicy</td>
<td>ALLOW</td>
</tr>
</tbody>
</table>

allows all the traffic to and from gateways that match BLRBLD1GeolocPolicy to and from VoIP phones that match BLRBLD1GeolocPolicy.

If more granular policies are required, the geolocation NAM field allows naming the devices within a building.

Example

- Between desktop phones and gateway1 in BLD1 of Bangalore
  
  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=deskphone)
  
  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=gateway1) = Allow

- Between Cisco IP Softphones and ICT1 in BLD1 of Bangalore
  
  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=softphone)
  
  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=ICT1) = Allow

Devices that have geolocation fields that match the preceding policies can communicate as per policy. See the “Logical Partitioning Policy Configuration” section on page 32-40 for details of how to use Cisco Unified Communications Manager Administration to configure logical partitioning policies.

Additional Information

See the “Related Topics” section on page 32-47.
LPPolicyManager and Policy Tree

LPPolicyManager specifies a singleton process that interfaces with database and maintains policies in call processing as logical partitioning policy tree. During Cisco Unified Communications Manager service startup, the LPPolicyManager reads the policies from database tables and constructs the logical partitioning policy tree.

The add/delete/update of a policy in the database results in change notification to LPPolicyManager, and the change takes place in the logical partitioning policy tree.

Call processing interfaces with LPPolicyManager to read the logical partitioning policies that correspond to the geolocation policy records for the devices.

The LPPolicyManager provides utility functions for these search types:

- Geolocation information for a pair of devices
- Geolocation information for existing devices versus a new participant
- Geolocation information for existing devices versus list of new participants

Policy Tree Example

This section presents examples of a policy tree.

Figure 32-1 provides an example of a policy tree for logical partitioning policies for India cluster between geolocation policy records for gateways in Bangalore (BLD1, BLD2) and VoIP phones in Bangalore (BLD1, BLD2).

Note

Normally, only one pair of policies gets configured between a particular source geolocation policy record and a particular target geolocation policy record.

The policy tree gets constructed so that a paired policy is represented as a source and target portions on the tree.

For example, the policy records with data Src=Border:IN:KA:Bangalore:BLD1 and Target=Interior:IN:KA:Bangalore:BLD1 with policy Allow associate with the following nodes:

- Border, IN, KA, Bangalore, BLD1 in the source portion
- Interior, IN, KA, Bangalore, BLD1 in the target portion

For this example, the Allow policy gets configured in the leaf node of the target portion.

The figure shows that the target portion of the tree can have a possible policy at each level. That is, each node (Interior, IN, KA, Bangalore, and BLD1) can have a policy.
See the “Logical Partitioning Policy Search Algorithm” section on page 32-15 for a discussion of the logical partitioning policy search algorithm for searching through a policy tree. Table 32-3 on page 32-16 provides a listing that shows all permutations of possible policies that are found in this example policy tree.

**Policy Tree Construction**

The policy tree construction follows a fixed algorithm. The policy tree includes a source portion and a target portion.

1. [GLP_X Border GLP_Y Interior] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

2. [GLP_Y Interior GLP_X Border] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

Thus, the Border-to-Interior policy specifies that the Border part always originates in the source portion of the tree. The policy gets added in a leaf node.

3. [GLP_X Border GLP_Y Border] policy gets added.

First, a determination decides whether to add GLP_X in the source portion or GLP_Y in the source portion.
If no existing policy matches any tokens of GLP_X or GLP_Y (due to other GLP policy), the tree construction takes the source portion from GLP_X Border and the target portion from GLP_Y Border.

If an existing policy matches some tokens in the source portion, the source portion gets taken from that GLP.

**Example 1:** GLP_Y Border GLP_X Interior is already configured.

Because GLP_Y is already used in the source portion, to add the [GLP_X Border GLP_Y Border] policy, the GLP_Y gets added in the source portion.

**Example 2:** If the two policies, [GLP_X Border GLP_Y Interior] and [GLP_Y Border GLP_X Interior] exist, two source branches exist that both start with Border.

Assume that GLP_B overlaps more tokens with GLP_X (as compared to GLP_Y) and GLP_A does not match any Border branches.

To add the [GLP_A Border GLP_B Border] policy, the policy gets searched as to whether GLP_A or GLP_B can fit in the existing source branches.

As GLP_B matches some tokens from GLP_X, the portion of the tree gets shared with GLP_X.


Thus, for Border-to-Border policies, the policy tree gets constructed to fit best in the existing source and target branches. Consider sharing as many nodes as possible as preferable.

**Additional Information**

See the “Related Topics” section on page 32-47.

---

**Logical Partitioning Policy Search Algorithm**

This section explains the logical partitioning policy search algorithm.

The logical partitioning policy search algorithm functions as follows:

- Policies get searched during call control or feature interactions.
- The configured tree of policies gets used for run-time searching of the configured policy by using tree traversal.
- The policy gets searched between a pair of devices by using geolocation information (that is, geolocation, geolocation filter, and device type) of both the source (A) device and target (B) device.

**Basic Operation**

Construct a list of name/value pairs from the geolocation and geolocation filter information (that is, pairList1 and pairList2).

**Example:** pairList = "Country=IN;A1=KA;A3=Bangalore;LOC=BLD1"

Input for the search specifies {pairList1, devType1}, {pairList2, devType2}.

The following steps take place during the policy search:

**Step 1**

If devType1=Border and devType2=Interior, set {devTypeA=devType1, pairListA= pairList1} and {devTypeB=devType2, pairListB= pairList2}.
Step 2  If devType1=Interior and devType2=Border, set \{devTypeA=devType2, pairListA= pairList2\} and \{devTypeB=devType1, pairListB= pairList1\}.

Step 3  Match the exact pair by searching the nodes of a policy tree. Use values from \{devTypeA, pairListA\} and find the source branch of the tree.

Step 4  Use values from \{devTypeB, pairListB\} and find the target (paired) branch of the tree.

Step 5  If an exact match is found in the tree and the policy is configured, use the policy data that is configured in the leaf node and return the policy value.

Step 6  If exact match is not found, find a match by stripping one column from pairListB input (that is, go one level up on target [paired] branch of policy tree and check whether policy data is configured in the corresponding node).

Step 7  If a match is found, return the policy value; otherwise, continue going up the paired branch of the policy tree and check whether policy data is configured.

Step 8  If a policy is not found, go one level (node) up on the source branch that corresponds to pairListA.

Step 9  Repeat Step 4 through Step 8 until a policy is found or the root node is reached.

Step 10 If devType1=Border and devType2=Border, search for exact match by traversing. Use \{devTypeA=devType1, pairListA= pairList1\}, and \{devTypeB=devType2, pairListB= pairList2\}. If not found, traverse and use \{devTypeA=devType2, pairListA= pairList2\} and \{devTypeB=devType1, pairListB= pairList1\}.

*Note*  The tree layout can specify any order, based on how the administrator added policies, so you need to use both combinations to search the tree.

Assume that the policy is searched with the following data:


In Table 32-3 that shows all permutations of possible policies, any value specifies a match. The search algorithm proceeds in the order that the table specifies for finding the configured policy. The first found match specifies an entry from which the configured policy gets used.

**Table 32-3  Example of Policy Variations in Policy Configuration and Order of Policy Search**

<table>
<thead>
<tr>
<th>GeolocationValueA</th>
<th>GeolocationValueB</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Border:IN:KA:Bangalore:BLD1</td>
<td>Interior:IN:KA:Bangalore:BLD1</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore:BLD1</td>
<td>Interior:IN:KA:Bangalore</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore:BLD1</td>
<td>Interior:IN:KA</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore:BLD1</td>
<td>Interior:IN</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA:Bangalore:BLD1</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA:Bangalore</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA:Bangalore:BLD1</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA:Bangalore</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior:IN:KA</td>
<td>Allow/Deny</td>
</tr>
<tr>
<td>Border:IN:KA:Bangalore</td>
<td>Interior</td>
<td>Allow/Deny</td>
</tr>
</tbody>
</table>
Policy Matching

Policy checking takes place in the following situations:

- Policy checking occurs for all calls that connect a PSTN gateway and a VoIP phone.
- Policy checking occurs for all calls that invoke supplementary services, such as Transfer and Conference, that connect a PSTN gateway and VoIP phones.
- All restricted calls and connections based on policies get denied.

Additional Information

See the “Related Topics” section on page 32-47.
Deny Policy Handling

When calls are denied because of logical partitioning policy, the following handling occurs:

- Basic calls get cleared with a reorder tone that Cisco Unified Communications Manager sends.
  - Q.850-compliant devices (SCCP, H323. MGCP) get cleared by using cause code=63 “Service or option not available.”
  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- Features get handled based on the individual feature
  - If call clearing is involved, the cause code=63 or SIP status code=503 gets used.
  - Feature-based message gets sent to VoIP phones for display on the status line.
  - For analog phones that invoke a feature, Transfer results in both calls getting cleared. Conference clears the secondary call to play reorder tone to the analog phone.

Additional Information
See the “Related Topics” section on page 32-47.

LPSession Infrastructure and Policy Checking

LPSession specifies an infrastructure that enhances the Cisco Unified Communications Manager Resource Reservation Protocol (RSVP) infrastructure to provide a centralized policy-checking infrastructure.

The enhancement of the RSVP infrastructure is based on similar paired policy checking behavior for logical partitioning. Logical partitioning has no impact on RSVP policy checking and vice-versa.

The following operations use LPSession infrastructure for policy checking:

- Basic calls
- Redirections (for example, Forwarding, Redirecting features, and Park reversion)
- Split/Join primitive

The commonly used features perform logical partitioning policy checks in the feature layer before Split/Join or Redirection:

- Transfer
- Ad Hoc Conference
- Meet-me Conference
- Pickup
- Call Park and Directed Call Park

Other existing Split/Join features and similar features depend on LPSession infrastructure for Split/Join primitive-level policy checking (for example, MKI for Cisco Unified Mobility).

Additional Information
See the “Related Topics” section on page 32-47.
Logical Partitioning Handling for a Basic Call

This section describes logical partitioning handling with a basic call.

**Operation**
The logical partitioning policy gets checked between the geolocation policy records of the calling device and the called device.

**Configuration**
The calling device and the called device both associate with a geolocation and geolocation filter.

**When**
Logical partitioning handling takes place in the following circumstances:

- During a basic call between a VoIP phone and a PSTN gateway, a PSTN gateway and another PSTN gateway, an ICT and a PSTN gateway, or an ICT and another ICT.
- During Post Digit Analysis, which uses configured calling search spaces and partitions for routing the calls.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

**When Not**
Logical partitioning handling does not take place in the following circumstances:

- When both the calling and called devices specify VoIP phones (DevType=Interior).
- When geolocation or geolocation filter is not associated with any device.

**Deny Handling**
Logical partitioning handles a denied call as follows:

- The call gets denied/rejected with a reorder tone.
- The call does not get extended to a phone, gateway, or intercluster trunk.
- The Number of Basic Call Failures perfmon counter gets incremented.

**Additional Information**
See the “Related Topics” section on page 32-47.

Logical Partitioning Interaction with Geolocation Conveyance Across SIP Trunks and Intercluster Trunks

If logical partitioning applies to a multicluster environment, ensure location conveyance is configured. Location conveyance configuration entails the same configuration as logical partitioning configuration for a single-cluster environment, but additional configuration must take place for devices that belong to remote clusters.
For the details of configuring logical partitioning for systems that do not require location conveyance, see the “Configuration Checklist for Logical Partitioning” section on page 32-1.

To support logical partitioning scenarios that involve participants across clusters requires the following support from SIP trunks and intercluster trunks:

- The geolocation and device type information gets sent from one cluster to another cluster.
- This information gets sent both at call establishment and at midcall joins and redirects.
- The geolocation filter gets configured on the trunk.
  - This configuration allows creation of geolocation identifiers. Based on these geolocation identifiers, policy records may be configured for logical partitioning policy checks.

The geolocation gets sent across clusters if the Send Geolocation Information check box gets checked upon configuration of the SIP trunk or intercluster trunk:

- If geolocation is configured for a device, the geolocation information gets sent in call signaling across the trunk for SIP trunk or intercluster trunk interactions.

**Note**

Location conveyance does not depend on any logical partitioning configuration.

For additional details, see the “Geolocation Conveyance Across SIP Trunks and Intercluster Trunks” section on page 24-22.

The “Configuration Checklist for Location Conveyance” section on page 24-4 provides a detailed checklist for configuring location conveyance.

**Additional Information**

See the “Related Topics” section on page 32-47.

**Logical Partitioning Handling of a Received Geolocation**

If the receiving cluster is enabled for logical partitioning, the receiving cluster uses the received PIDF-LO geolocation information for logical partitioning policy checks with the devices on Cisco Unified Communications Manager.

For additional details, see the “Handling a Received Geolocation” section on page 24-23.

Also, see the “Interactions” section on page 32-22 for a list of features that use geolocation information for policy checking.

**Additional Information**

See the “Related Topics” section on page 32-47.

**Logical Partitioning Feature Interactions with Midcall Geolocation Change**

If logical partitioning is enabled, the following actions take place:

- SIP trunk or intercluster trunk checks the logical partitioning policy and takes an action that is based on the configured policy.
- The feature layer, such as Conference or Meet-me, rechecks the logical partitioning policy based on the updated geolocation information for the trunk device.

For feature interactions that involve a midcall geolocation change, see the “Feature Interactions with Midcall Geolocation Change” section on page 24-23.
Also, see the “Interactions” section on page 32-22 for a list of features that use geolocation information for policy checking.

**Additional Information**
See the “Related Topics” section on page 32-47.

### Dynamic SIP Trunks

For dynamic SIP trunks, such as Cisco Intercompany Media Engine (IME), Service Advisement Framework (SAF), or Cisco Extension Mobility Cross Cluster (EMCC), the target cluster varies depending on the pointed destination. The device-level geolocation and geolocation filter that can be configured on these trunks may not have the flexibility to vary depending on the destination. Such SIP trunks must be configured appropriately to allow or deny traffic from these trunks. Cisco Systems recommends using location conveyance functionality, which allows the actual geolocation to propagate across clusters and helps in accurate logical partitioning policy checking.

**Additional Information**
See the “Related Topics” section on page 32-47.

### SIP Trunk or Intercluster Trunk Configuration Requirement for Logical Partitioning

A cluster for which logical partitioning is enabled exhibits the following typical behaviors:

1. Traffic between VoIP phones and SIP trunk (or intercluster trunk [ICT]) gets allowed.
2. Traffic between SIP trunk (or ICT) and PSTN gateways gets blocked.
3. VoIP-only traffic between SIP trunk (or ICT) and SIP trunk (or ICT) gets allowed.

Logical partitioning policies must get configured to achieve these behaviors.

**Interaction with Non-Location Conveyance Cluster**

To achieve behaviors 1 and 3, you need to configure one policy each. If default policy specifies Deny, you do not need any policy for behavior 2.

For behaviors 1 and 3, because no location conveyance exists, a logical partitioning cluster cannot identify whether traffic is VoIP-only or comes from a gateway in a remote cluster. This means that typically, all traffic must be allowed from SIP trunk (or ICT) to VoIP phones or other SIP trunk (or ICT).

**Interaction with Location Conveyance Cluster**

For behavior 1, the VoIP phone that calls a SIP trunk (or ICT) needs a policy that allows extension of the call on the trunk. This occurs before receipt of location conveyance information from the remote cluster.

For incoming VoIP call from SIP trunk (or ICT), you do not need any policy for calling VoIP phones. If traffic from SIP trunk (or ICT) needs to be allowed to any other ICT or PSTN gateway, you require a corresponding policy.

**Example**

Ensure the SIP trunk that points from Bangalore to RCDN cluster is configured as follows:

- Geolocation = “IN:KA:Bangalore:ICTToRCDN”
- Geolocation Filter = “UseCountry, UseA1, UseA3, UseNam”
This configuration specifies the geolocation identifier for SIP trunk as follows:

{"IN:KA:Bangalore:ICTToRCDN", devType=Border}

Configure logical partitioning policies as follows:

“Border:IN:KA:Bangalore:ICTToRCDN” to Interior = Allow

**Result:** All VoIP phones in Bangalore cluster can communicate with Richardson.


**Result:** ICTs can communicate.

These policies fulfill behavior 1 and 3 requirements.

For location conveyance scenarios, ensure the policies are configured based on geolocation configurations and device type for devices across the cluster.

**Additional Information**

See the “Related Topics” section on page 32-47.

## System Requirements for Logical Partitioning

Logical partitioning requires the following software components:

- Cisco Unified Communications Manager 7.1 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer 7 or Microsoft Internet Explorer 8 or FireFox 3.x or Safari 4.xr

**Additional Information**

See the “Related Topics” section on page 32-47.

## Interactions and Limitations

The following sections describe the interactions and restrictions for logical partitioning:

- Interactions, page 32-22
- Limitations, page 32-37

**Additional Information**

See the “Related Topics” section on page 32-47.

## Interactions

The following sections detail the interactions between logical partitioning and the supplementary features and call processing entities that are listed.
Configure the Logical Partitioning Default Policy enterprise parameter, and configure a corresponding logical partitioning policy through the Call Routing > Logical Partitioning Policy Configuration menu option.

- Call Forwarding, page 32-23
- Call Transfer, page 32-24
- Ad Hoc Conference, Join, Join Across Lines (JAL), page 32-27
- Meet-Me Conference, page 32-28
- Call Pickup, page 32-29
- Call Park and Directed Call Park, page 32-30
- Cisco Extension Mobility, page 32-31
- Cisco Unified Mobility, page 32-32
- Shared Line, page 32-33
- Barge, cBarge, and Remote Resume, page 32-34
- Route Lists and Hunt Pilots, page 32-35
- CTI Handling, page 32-36

Logical partitioning also interacts with the following Cisco Unified Communications Manager components:

- Bulk Administration Tool—For information on how the Bulk Administration Tool (BAT) supports logical partitioning, see the Cisco Unified Communications Manager Bulk Administration Guide.
- Call Detail Records—For logical partitioning failures, existing call termination cause codes and new Cisco-specific call termination cause codes get used. For more information on CDRs, see the Cisco Unified Communications Manager Call Detail Records Administration Guide.
- Real Time Monitoring Tool—The Real Time Monitoring Tool provides a set of performance monitoring (perfmon) counters for the Cisco Call Restriction object that increment in the event of logical partitioning failures. The Real Time Monitoring Tool also tracks a Logical Partitioning Failures Total counter in the Call Activity window. For more information on the Real Time Monitoring Tool, see the Cisco Unified Real Time Monitoring Tool Administration Guide.
- Cisco Unified Reporting—Cisco Unified Reporting generates reports that provide information about logical partitioning policies. For more information on the reports that Cisco Unified Reporting generates, see the Cisco Unified Reporting Administration Guide.

Additional Information
See the “Related Topics” section on page 32-47.

Call Forwarding

This section describes the interaction of logical partitioning with the Call Forwarding feature.

Operation
The logical partitioning policy check gets performed between the geolocation identifier of the device from which call is coming and the device to which the call is forwarded.
Chapter 32      Logical Partitioning

Configuration

The caller device and a forwarded device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When an incoming call is received for a device that is call forwarded to another device, the Forwarding feature invocation takes place.
- One of the devices specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and forwarded Cisco Unified Communications Manager devices for performing logical partitioning policy checking.
- The configured logical partitioning policy returns to the forwarded Cisco Unified Communications Manager device, which takes action accordingly.
- This handling applies to all variations of call forwarding; for example, Call Forward All (CFwdAll), Call Forward No Answer (CFNA), and Call Forward Busy (CFB).

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and forwarded devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The calling device receives a reorder tone from Cisco Unified Communications Manager.
  - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”

Additional Information

See the “Related Topics” section on page 32-47.

Call Transfer

This section describes the interaction of logical partitioning with the Call Transfer feature.

Operation

The logical partitioning policy check gets performed between the geolocation identifier of the device that is acting as a transferred party and the geolocation identifier of the device that is acting as a transferred destination.

Configuration

The transferred device and a transferred destination device associate with a geolocation and geolocation filter.
When
Logical partitioning handling takes place in the following circumstances:

- When a phone uses a Transfer softkey to transfer the call, the second Transfer key press results in Transfer feature invocation and processing.
- Similarly, other mechanisms (for example, Direct Transfer, OnHook Transfer, Hook Flash Transfer, CTI-application-initiated Transfer) that result in Transfer feature invocation get included.
- The transferred or/and transferred destination specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the transferred and transferred destination Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- This handling normally gets performed before splitting of the primary and secondary calls and before joining.

When Not
Logical partitioning handling does not take place in the following circumstances:

- When both the Transferred and Transferred Destination devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling
Logical partitioning handles a denied call as follows:

- Sends External Transfer Restricted message to the VoIP phone.
- Normal Transfer—For phone that is running SCCP, the primary call remains on hold, and consultation call remains active. For phone that is running SIP, both primary and consultation calls remain on hold and need to be resumed manually after the failure.
- Onhook, HookFlash and Analog-Phone-Initiated Transfer—Both the primary and secondary calls get cleared by using cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager.
- The Number of Transfer Failures perfmon counter gets incremented.

Interaction with Block OffNet to OffNet Transfer Service Parameter
The Block OffNet to OffNet Transfer service parameter allows the Transfer feature to block the transfer operation when both Transferred and Transferred Destinations specify offnet calls.

See the “Setting the Block OffNet to OffNet Transfer Service Parameter” section on page 23-7 in the “External Call Transfer Restrictions” chapter of this guide for more information about this service parameter.

The Cisco Unified Communications Manager cluster that is disabled for logical partitioning retains the expected behavior that this service parameter specifies.

Logical Partitioning-Enabled Cluster
In a logical partitioning-enabled Cisco Unified Communications Manager cluster, you can configure the system to allow multiple Voice Gateway (PSTN) participants that use the GeolocationPolicy, GLPolicyX, in a supplementary feature by configuring a policy such as the following one:

```
GLPolicyX Border GLPolicyX Border Allow
```
After Cisco Unified Communications Manager configures such a policy, be aware that all features (such as Forwarding, Transfer, Ad Hoc Conference, and so forth) are allowed between participants that use GeolocationPolicy, GLPolicyX Border. For example, forwarding a call that comes from a party that uses GLPolicyX Border to another party that uses GLPolicyX Border gets allowed.

Assume that Cisco Unified Communications Manager deployment requires that all supplementary features except the Transfer feature function for such participants. If so, the Block OffNet to OffNet Transfer service parameter can block transfer between offnet devices even if the logical partitioning policy is allowed.

This service parameter controls only the blocking of offnet-to-offnet transfers and does not impact any other supplementary features. Thus, the following details highlight scenarios that involve voice-gateway-to-voice-gateway transfers.

Details

1. **Border-to-Border Logical Partitioning Policy Specifies Deny**
   
   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager denies the transfer. The “External Transfer Restricted” message displays to the transferring party.
   
   The Cisco Unified Communications Manager setting (either True or False) for the Block OffNet to OffNet Transfer service parameter does not affect the Transfer operation.
   
   The logical partitioning Deny policy takes precedence, and Cisco Unified Communications Manager follows the policy strictly.

2. **Border-to-Border Logical Partitioning Policy Specifies Allow**

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager checks the allow policy and also checks the setting of the Block OffNet to OffNet Transfer service parameter. This service parameter thus affects the transfer between offnet participants.
   
   a. Block OffNet to OffNet Transfer service parameter specifies True—Cisco Unified Communications Manager checks whether both parties (transferred and transferred destination) are offnet. If so, the transfer of such calls gets denied, and the “External Transfer Restricted” message displays to the transferring party.
   
   Because transfer gets blocked due to the service parameter, the serviceability Perfmon counter for Logical Partitioning Transfer Failures does not increment.
   
   b. Block OffNet to OffNet Transfer service parameter specifies False—Transfer succeeds.

**Offnet/Onnet Behavior for a Device**

For outgoing calls, the Call Classification setting in the Route Pattern Configuration window determines the offnet or onnet value. The Call Classification value in the Route Pattern Configuration window overrides the device-level configuration or the corresponding value of the Call Classification service parameter.

For incoming calls, the device-level configuration or the corresponding Call Classification service parameter value determines the offnet or onnet value.

**Additional Information**

See the “Related Topics” section on page 32-47.
Ad Hoc Conference, Join, Join Across Lines (JAL)

This section describes the interaction of logical partitioning with the Ad Hoc Conference, Join, and JAL features.

**Operation**

Establishing Conference—The logical partitioning policies get checked between the geolocation identifiers of the devices that are invited to an ad hoc conference.

Established Conference—The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the conference and the device that is invited to the conference.

**Configuration**

The participant devices associate with a geolocation and a geolocation filter.

The conference bridge does not need to associate with geolocation or geolocation filter; only participants associate, and policy checks get performed for the participants.

**When**

Logical partitioning handling takes place in the following circumstances:

- A phone uses a Conference softkey to establish or extend an ad hoc conference or a CTI application initiates ad hoc conference.
- The second Conference key press results in conference feature invocation and processing.
- Cisco Unified Communications Manager uses participant geolocation identifier information for policy checking.
- In an established conference, policy checking occurs again, based on changed participant geolocation identifier information for midcall updates. For example, policy checking occurs during call state change, such as Alerting to Answer, Hold/Remote-Resume, Transfer, Call Park Retrieval, Redirection, and so forth.
- PSTN participants are involved.

**When Not**

Logical partitioning handling does not take place in the following circumstances:

- When all participants are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

**Deny Handling**

Logical partitioning handles a denied conference as follows:

- For the establishing-conference case, the CFB does not get allocated.
- For phones that are running SCCP or phones that are running SIP, the primary call leg gets put on hold and the consultation call remains active. If the primary call leg needs to resume, resumption must take place manually.
- The Conference is Unavailable message gets sent to the VoIP phone that initiates the conference.
• When an analog phone initiates the conference, the secondary call gets cleared by using cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager.
• The Number of Adhoc Conference Failures perfmon counter increments.

Additional Information
See the “Related Topics” section on page 32-47.

Meet-Me Conference

This section describes the interaction of logical partitioning with the Meet-Me Conference feature.

Operation
The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the meet-me conference and the device that is attempting to join the conference.

Configuration
The participant devices associate with a geolocation and a geolocation filter.
Be aware that the conference bridge is not required to be associated with a geolocation or geolocation filter; only participants get associated, and policy checks get performed for the participants.

When
Logical partitioning handling takes place in the following circumstances:
• Requirement exists for PSTN participant involvement.
• Policy checks get supported during joining of participants. When a participant dials the meet-me number to join in a meet-me conference, the participant geolocation gets used for policy checking before the new participant is allowed to join the meet-me conference.
• In an established meet-me conference, the updated policy of the participant gets used for policy checking during midcall updates (such as Hold-Resume, Transfer, Barge, cBarge, Call Park Retrieval, and so forth).

When Not
Logical partitioning handling does not take place in the following circumstances:
• When all participants are VoIP phones (DevType=Interior), handling does not occur.
• When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

Deny Handling
Logical partitioning handles a denied call as follows:
• The MeetMe is Unavailable message gets sent to the VoIP phone.
• The existing conference does not get affected.
• The call gets cleared with reorder tone from Cisco Unified Communications Manager.
  – Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
- SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Meet-Me Conference Failures perfmon counter increments.

Additional Information
See the “Related Topics” section on page 32-47.

Call Pickup

This section describes the interaction of logical partitioning with the Call Pickup feature.

Operation
The logical partitioning policies get checked between the geolocation identifiers of the calling device and that of the device that picks up the call.

Configuration
The calling device and the device that attempts pickup associate with a geolocation and a geolocation filter.

When
Logical partitioning handling takes place in the following circumstances:
- A PSTN device calls a VoIP phone (A) to which another VoIP phone (B) has a Pickup group relation (for example, both phones belong to the same pickup group).
- When phone B attempts pickup by pressing either Pickup, OPickup, Group Pickup, or BLF Pickup button, the Pickup feature gets invoked.
- Cisco Unified Communications Manager uses geolocation identifier information of the calling device and of device picking up call for policy checking.
- When only one alerting call occurs, the corresponding logical partitioning policy gets treated as final.
- When multiple alerting calls occur, the logical partitioning policy gets checked for each alerting call, starting from the longest alerting call until logical partitioning policy is allowed and call is picked up. If last processed alerting call has logical partitioning Deny policy and no more alerting calls occur, deny handling action takes place.

When Not
Logical partitioning handling does not take place in the following circumstances:
- When the caller consists of a VoIP phone (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.

Deny Handling
Logical partitioning handles a denied pickup as follows:
- PickUp is Unavailable message gets sent to the VoIP phone that attempts pickup.
- The alerting call does not get affected.
- For multiple alerting calls (mixture of Allowed and Deny policy), if a call with deny policy fails for pickup first, Cisco Unified Communications Manager proceeds by picking up the next alerting call.
Cisco Unified Communications Manager sends reorder tone to the phone that attempts the pickup.
- Q.850-compliant devices (phone that is running SCCP) get cleared by using cause code=63 “Service or option not available.”
- SIP phone gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Pickup Failures perfmon counter increments.

Additional Information
See the “Related Topics” section on page 32-47.

Call Park and Directed Call Park

This section describes the interaction of logical partitioning with the Call Park and Directed Call Park features.

Operation
The logical partitioning policies get checked between the geolocation identifier of the device that is retrieving the call and the geolocation identifier of the parked party.

Configuration
For Retrieval—The parked party and the device that attempts park retrieval associate with a geolocation and geolocation filter.
For Reversion—The parked party and device to which reversion happens associate with a geolocation and geolocation filter.

When
Logical partitioning handling takes place in the following circumstances:
- When a parked call exists and a device attempts a park retrieval, the Park retrieval feature gets invoked.
- When a parked call exists and the reversion timer expires, the Park reversion feature gets invoked.
- One party must be a PSTN participant.
- For Park retrieval, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device that performs park retrieval for policy checking.
- For Park reversion, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device to which call is redirected for policy checking.

When Not
Logical partitioning handling does not take place in the following circumstances:
- When the involved devices are VoIP phones (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.
Deny Handling
Logical partitioning handles a denied retrieval/reversion as follows:

- For retrieval, Cannot Retrieve Parked Call message gets sent to the VoIP phone.
- Cisco Unified Communications Manager sends reorder tone to the phone that is attempting retrieval.
  - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
  - Phone that is running SIP or SIP trunk gets cleared by using SIP status code=503 “Service unavailable.”
- For reversion, the parked call gets cleared with reorder tone.
- The Number of Park Retrieval Failures perfmon counter gets incremented (for both Call Park and Directed Call Park retrievals that get denied).

Additional Information
See the “Related Topics” section on page 32-47.

Cisco Extension Mobility

This section describes the interaction of logical partitioning with the Cisco Extension Mobility feature.

Operation
A user logs on to a VoIP phone by using Cisco Extension Mobility within the same Cisco Unified Communications Manager cluster. The incoming or outgoing calls from the phone get logical partitioning policy checked.

Configuration
The VoIP phone that is logged on to Cisco Extension Mobility and the PSTN access device both associate with a geolocation and geolocation filter.

When
Logical partitioning handling takes place in the following circumstances:

- A user logs on, by using Cisco Extension Mobility, to a device in a different geolocation as the device profile, and the user makes a PSTN call by using a gateway in the user home site, or the user receives an incoming PSTN call.
- Cisco Unified Communications Manager uses geolocation identifier information of the Cisco Extension Mobility logged-on device and the PSTN gateway device for policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not
Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with a VoIP phone that is logged on to Cisco Extension Mobility nor with the calling party nor called party device.
- The VoIP phone that is logged on to Cisco Extension Mobility calls or receives a call from a VoIP phone (DevType=Interior).
Deny Handling
Logical partitioning handles a denied call as follows:
- If the VoIP phone that is logged in to Cisco Extension Mobility places a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.
- If the VoIP phone that is logged in to Cisco Extension Mobility receives a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.

Additional Information
See the “Related Topics” section on page 32-47.

Cisco Unified Mobility
This section describes the interaction of logical partitioning with the Cisco Unified Mobility feature. These interactions apply to calls that involve Mobile Connect or Mobile Voice Access.

Operation
Logical partitioning interacts with Cisco Unified Mobility as follows:
- Single-Number-Reach (SNR) Call—The SNR call gets logical partitioning policy checked between a calling device and a PSTN gateway that connects the mobile device.
- Cell Pickup—The Cell Pickup operation from a desktop phone attempts to join the already connected call with a PSTN gateway that connects the remote destination mobile device. The logical partitioning policy gets checked before joining the call by using the geolocation identifiers for the involved devices.
- Mobile Voice Access—The logical partitioning policy gets checked between the geolocation identifier of the incoming gateway and the geolocation identifier of the called party device.

Configuration
The involved devices and the PSTN access gateway must associate with a geolocation and geolocation filter.

When
Logical partitioning handling takes place in the following circumstances:
- Single-Number-Reach (SNR) Call
  Cisco Unified Mobility gets configured for an enterprise extension, and a call is received for SNR from a VoIP phone or another PSTN gateway.
  Cisco Unified Communications Manager uses the geolocation identifier information that associates with calling and called Cisco Unified Communications Manager device to perform logical partitioning policy checking.
  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.
- Cell Pickup
  Cisco Unified Mobility gets configured for an enterprise extension, and a call is active between a VoIP phone (SNR) and another VoIP phone or a PSTN gateway (termed the connected party).
  The VoIP phone (SNR) performs Cell Pickup to Mobile, which tries to join the connected party with the PSTN gateway that was used to reach the mobile phone.
Cisco Unified Communications Manager uses the geolocation identifier information that associates with the PSTN gateway and the connected party for performing logical partitioning policy checking. The configured logical partitioning policy decides whether the Cell Pickup operation succeeds or fails.

- **Mobile Voice Access**
  Cisco Unified Mobility gets configured for an enterprise extension, and a mobile phone calls from a PSTN gateway to an enterprise VoIP phone.
  Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and called VoIP phone to perform logical partitioning policy checking.
  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

**When Not**
Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with the involved devices.
- No logical partitioning support exists when a dual-mode phone is used.

**Deny Handling**
Logical partitioning handles a denied call as follows:

- For SNR and Mobile Voice Access, the call gets cleared or rejected with a reorder tone.
- For cell pickup, the original call between connected party and VoIP phone (SNR) gets restored, and the Cannot Send Call to Mobile message displays on the VoIP phone.

**Additional Information**
See the “Related Topics” section on page 32-47.

**Shared Line**

This section describes the interaction of logical partitioning with the Shared Line feature.

**Operation**
The call to or from a shared line uses the same processing for logical partitioning checks as a basic call.
The shared-line device on Cisco Unified Communications Manager performs logical partitioning policy checks for displaying remote-in-use (RIU) information. The policy gets checked between the geolocation identifier for the connected party and the shared-line device that shows RIU information.

**Configuration**
The shared-line devices and the PSTN access device (a VoIP gateway) associate with a geolocation and geolocation filter.

**When**
Logical partitioning handling takes place in the following circumstances for a basic call:

- A shared line exists for the VoIP phones that span different geolocations, and one of the VoIP phones makes or receives a PSTN call through its local PSTN gateway.
For completing the call from a shared line to a PSTN gateway, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling shared-line phone and with the called PSTN gateway to perform logical partitioning policy checking.

For completing the call from a PSTN gateway to a shared line, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and with each of the called shared-line phones to perform logical partitioning policy checking.

The configured logical partitioning policy gets returned to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

For determining whether to display the remote-in-use (RIU) information, Cisco Unified Communications Manager uses the geolocation identifier information of each device that associates with the shared line and that of the connected party (calling or called) to perform logical partitioning policy checking.

When Not
Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), no handling occurs.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.

Deny Handling
Logical partitioning handles a denied call as follows:

- Cisco Unified Communications Manager drops the call (or does not extend the call) to the called shared-line devices that are in unauthorized geolocations for the calling device.
- The call instance information does not display on the shared-line device in the remote-in-use state.

Additional Information
See the “Related Topics” section on page 32-47.

Barge, cBarge, and Remote Resume

This section describes the interaction of logical partitioning with the Barge, cBarge, and Remote Resume features.

Operation
The Barge, cBarge, or Remote-Resume operations on a shared line depend on the availability of call instance information in the remote-in-use (RIU) state.

The same logical partitioning policy checks that apply to shared-line interactions determine the availability of RIU information.

For logical partitioning deny cases, the RIU call instance gets withdrawn on a restricted shared line.

Configuration
The shared-line devices and the PSTN access device associate with a geolocation and geolocation filter.
When
Logical partitioning handling takes place in the following circumstances:

- A shared line exists for the VoIP phones that span different geolocations and one VoIP phone makes or receives a PSTN call through its local PSTN gateway.
- The display of remote-in-use (RIU) information gets handled as in the shared-line call scenario.
- During Hold for an active call by a shared-line device, no Remote Resume button is available.
- Because Barge and cBarge buttons are not available, these scenarios remain impossible.

When Not
Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), logical partitioning policy checks get ignored.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.
- When the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

Deny Handling
Logical partitioning handles a denied call as follows:

- The call instance information does not display.

Additional Information
See the “Related Topics” section on page 32-47.

Route Lists and Hunt Pilots

This section describes the interaction of logical partitioning with route lists and hunt pilots.

Operation
For route lists, the call from a device to gateways or MGCP ports that belong to route lists and route groups gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

For hunt pilots, the call from a PSTN device to a line device that belongs to a hunt list or hunt group gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

Configuration
The calling party and called party devices associate with a geolocation and geolocation filter.

When
Logical partitioning handling takes place in the following circumstances:

- A basic call takes place from a VoIP phone or a PSTN gateway through a route list to a PSTN gateway.
• A basic call takes place from a PSTN gateway through a hunt list to a set of VoIP phones.
• Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager devices to perform logical partitioning policy checking.
• The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

**When Not**
Logical partitioning handling does not take place in the following circumstances:
• When both the calling party and called party devices specify VoIP phones (DevType=Interior), handling does not occur.
• All devices must associate with both a geolocation and geolocation filter. If any device does not associate with both geolocation and geolocation filter, handling does not occur.

**Deny Handling**
Logical partitioning handles a denied call as follows:
• The call gets cleared or rejected with a reorder tone from Cisco Unified Communications Manager.

**Additional Information**
See the “Related Topics” section on page 32-47.

**CTI Handling**
This section describes the CTI interaction of logical partitioning with all features that perform Join or Redirects.

**Operation**
All the operations involving calls, joins, or redirects to a PSTN gateway get logical partitioning policy checked, and a CTI error gets generated for logical partitioning failures in the following instances:
• Basic call
• Transfer
• Conference
• Park retrieval and similar functions

**Configuration**
The involved devices associate with a geolocation and geolocation filter.

**When**
Logical partitioning handling takes place in the following circumstances:
• One of the devices specifies a PSTN participant.
• The logical partitioning policy gets checked in the context of an operation.
Chapter 32      Logical Partitioning

Interactions and Limitations

When Not
Logical partitioning handling does not take place in the following circumstances:

- When a geolocation or geolocation filter does not associate with any device, handling does not occur.
- When all the involved devices specify VoIP phones (DevType=Interior), handling does not occur.

Deny Handling
Logical partitioning handles a denied call by generating an operation-based CTI cause code as follows:

- Basic call—CTICMSIP503SERVICE NOT AVAILABLE.
- Redirection—CTIERR_REDIRECT_CALL_PARTITIONING_POLICY.
- Join, Transfer, Conference, and others.—CTIERR_FEATURE_NOT_AVAILABLE.

Additional Information
See the “Related Topics” section on page 32-47.

Limitations

The following limitations apply to logical partitioning:

- SIP trunk User Agent Server (UAS) location conveyance in UPDATE
  The UAS uses UPDATE request to communicate geolocation of the called party to the User Agent Client (UAC). This normally happens after 180 Ringing.
  The logical partitioning policy checks in logical partitioning-aware cluster that receives this geolocation may CANCEL the call if policy gets denied. A convenient end user experience may not occur.
- The logical partitioning checks do not get supported for participants across conferences in conference chaining.
  For example, meet-me and ad hoc chained conferences can have participants that are logical partitioning denied.
- Limitation with QSIG intercluster trunk (ICT)
  Be aware that the ICT with Q.SIG protocol is not allowed to communicate geolocation info for the caller or callee device. The ICT configuration for “Send Geolocation Information” gets disabled when the Q.SIG tunnelled protocol gets selected.
- Shared Line Active Call Info
  For logical partitioning restricted scenario, the shared line drops the active call information for the duration of the call, even if some feature moves the shared-line call to allowed category.
- cBarge/Barge
  Barge/cBarge does not occur because it gets prevented by not allowing shared lines to attempt these features based on logical partitioning deny policy with the connected party (the call instance gets dropped).
  However, when the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge.
feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

- Cisco Unified Communications Manager does not communicate geolocation info to H.323 or MGCP gateway.
  Communication to a SIP gateway can get disabled from a SIP trunk check box.

- Cisco Unified Communications Manager does not communicate geolocation information over a H.225 gatekeeper-controlled trunk.
  Scenario: Cisco Unified Communications Manager 1 remains logical partitioning enabled, but Cisco Unified Communications Manager 2 stays logical partitioning disabled.
  Phone A on CCM1 calls Phone B on CCM2 (using ICT or SIP trunk).
  Phone B presses conference and invites PSTN to conference.
  Limitation: The conference gets established.
  After phone B goes on hook, the call between phone A and the PSTN on Cisco Unified Communications Manager 2 gets cleared with a reorder tone.

- Mobility Cell Pickup: Logical partitioning Deny handling takes place after call gets answered on the mobile phone.
  The logical partitioning policy check does not happen before the call gets placed to the mobile phone (as it happens for a basic SNR call). The current design checks logical partitioning policy only after SsJoinReq processing, which takes place after the mobile phone answers the call.

- Cisco Extension Mobility logs in to a phone in a different geolocation
  Outgoing PSTN calls can occur when Local Route Groups are configured.
  Incoming PSTN calls do not get placed to the phone but receive a reorder tone.

- BLF SD or BLF Pickup Presence notifications do not get checked for logical partitioning policy.
  Currently, no logical partitioning infrastructure gets added for notifications.
  For forwarding failures, the RTMT Number of Forwarding Failures performance monitor counter does not increment. Instead, the Number of Basic Call Failures performance monitor counter increments.

- No reorder tone is provided on IOS H.323 and SIP gateways upon release of connected calls due to logical partitioning policies during supplementary features.

Example
Remote destination (RD) phone behind IOS SIP or H.323 gateway calls VoIP phone A.
After authentication completes, RD phone makes a call to phone C, but the call gets denied due to logical partitioning restricted policy.
Call gets cleared to RD phone with cause 63 (Service or option not available), but no reorder tone gets played to the RD phone.

Note
This cause code is common to all logical partitioning failure cases.

This behavior occurs due to a design limitation on the IOS gateway side, which does not play reorder tone after the CONNECT state. The only tones that play after the CONNECT state specify 17 (Busy) or 44 (No Circuit Available).
Similar limitations apply for Hook Flash, Onhook Transfer, and other supplementary features.
Configuring Logical Partitioning

This section contains information on the following topics:

- Geolocation Configuration, page 32-39
- Geolocation Filter Configuration, page 32-39
- Logical Partitioning Policy Configuration, page 32-40

Tip

Before you configure logical partitioning, review the “Configuration Checklist for Logical Partitioning” section on page 32-1.

Additional Information

See the “Related Topics” section on page 32-47.

Geolocation Configuration

Use the System > Geolocation Configuration menu option in Cisco Unified Communications Manager Administration to configure geolocations.

For details of geolocation configuration, see the “Geolocation Configuration” section on page 24-10.

Additional Information

See the “Related Topics” section on page 32-47.

Geolocation Filter Configuration

Use the System > Geolocation Filter menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

For details of geolocation filter configuration, see the “Geolocation Filter Configuration” section on page 24-17.

Additional Information

See the “Related Topics” section on page 32-47.
Logical Partitioning Policy Configuration

Use the Call Routing > Logical Partitioning Policy Configuration menu option in Cisco Unified Communications Manager Administration to configure logical partitioning policies.

To configure logical partitioning policies, see the following sections:

- Finding a Logical Partitioning Policy, page 32-40
- Configuring a Logical Partitioning Policy, page 32-41
- Deleting a Logical Partitioning Policy Record, page 32-42
- Deleting a Logical Partitioning Policy Pair Configuration, page 32-42
- Updating a Logical Partitioning Policy Pair Configuration, page 32-43
- Logical Partitioning Policy Configuration Settings, page 32-43

Additional Information

See the “Related Topics” section on page 32-47.

Finding a Logical Partitioning Policy

Because you might have multiple logical partitioning policies in your network, Cisco Unified Communications Manager lets you search for logical partitioning policies on the basis of specified criteria. Follow these steps to search for a specific logical partitioning policy in the Cisco Unified Communications Manager database.

Note

During your work in a browser session, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences until you modify your search or close the browser.

Procedure

Step 1

Choose Call Routing > Logical Partitioning Policy Configuration.

The Find and List Policies window displays. Records from an active (prior) query may also display in the window.

Step 2

To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.
Step 3  Click **Find**.

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

---

**Note**

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

---

Step 4  From the list of records that display, click the link for the record that you want to view.

---

**Note**

To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

---

**Additional Information**

See the “Related Topics” section on page 32-47.

---

**Configuring a Logical Partitioning Policy**

Perform the following procedure to add or update a logical partitioning policy.

**Procedure**

---

Step 1  Choose **Call Routing > Logical Partitioning Policy Configuration**.

The Find and List Policies window displays.

---

Step 2  Perform one of the following tasks:

- To add a new logical partitioning policy, click **Add New**.

  The Logical Partitioning Policy Configuration window displays.

- To update a logical partitioning policy, locate a specific logical partitioning policy as described in the “Finding a Logical Partitioning Policy” section on page 32-40.

---

Step 3  Enter the appropriate settings as described in **Table 32-4**.

---

Step 4  Click **Save**.

If you added a logical partitioning policy, the list box at the bottom of the window now includes the new logical partitioning policy.

---

**Additional Information**

See the “Related Topics” section on page 32-47.
Deleting a Logical Partitioning Policy Record

Perform the following procedure to delete an existing logical partitioning policy record.

Procedure

Step 1  Choose Call Routing > Logical Partitioning Policy Configuration. The Find and List Policies window displays.

Step 2  To locate a specific logical partitioning policy, enter search criteria and click Find. A list of geolocation filter logical partitioning policies that match the search criteria displays.

Step 3  Perform one of the following actions:

• Check the check boxes next to the logical partitioning policies that you want to delete and click Delete Selected.

• Delete all logical partitioning policies in the window by clicking Select All and then clicking Delete Selected.

• From the list, choose the name of the logical partitioning policy that you want to delete and click Delete.

A confirmation dialog displays.

Step 4  Click OK. The specified logical partitioning policy and all pair policies for this record get deleted.

Additional Information

See the “Related Topics” section on page 32-47.

Deleting a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

GLP-1 Border GLP-2 Interior Allow
GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be deleted, choose the second policy and select the Use Default Policy setting.

After you save, the corresponding pair of policies gets deleted from the matrix of policies.

Note that no change is made in the GLP-1 record.

Additional Information

See the “Related Topics” section on page 32-47.
Chapter 32  Logical Partitioning

Configuring Logical Partitioning

Updating a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

- GLP-1 Border GLP-2 Interior Allow
- GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be updated, choose the second policy and specify either Allow or Deny in the Policy setting.

After you save, the corresponding pair of policies gets updated from the matrix of policies.

Additional Information
See the “Related Topics” section on page 32-47.

Logical Partitioning Policy Configuration Settings

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

In the Logical Partitioning Policy Configuration window (Call Routing > Logical Partitioning Policy Configuration menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations.

Configure logical partitioning policies between pairs of geolocation policy records and device types. Ensure Allow and Deny policies are configured. See the “Allow and Deny Policies” section on page 32-6 for configuration details.

See the “Logical Partitioning Policies” section on page 32-11 for more information about logical partitioning policies, including examples.

Table 32-4 describes the configuration settings that are used for configuring logical partitioning policies.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Partitioning Policy</td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name (between 1 and 50 characters) for this logical partitioning policy. You may use all characters except quotes (&quot;), close angle bracket (&gt;), open angle bracket (&lt;), backslash (), ampersand (&amp;), and percent sign (%).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this logical partitioning policy.</td>
</tr>
<tr>
<td>Country</td>
<td>From the drop-down list box, choose a country for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A1</td>
<td>From the drop-down list box, choose an A1 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A2</td>
<td>From the drop-down list box, choose an A2 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A3</td>
<td>From the drop-down list box, choose an A3 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A4</td>
<td>From the drop-down list box, choose an A4 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A5</td>
<td>From the drop-down list box, choose an A5 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>A6</td>
<td>From the drop-down list box, choose an A6 value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>PRD</td>
<td>From the drop-down list box, choose a PRD value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>POD</td>
<td>From the drop-down list box, choose a POD value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>STS</td>
<td>From the drop-down list box, choose an STS value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>HNO</td>
<td>From the drop-down list box, choose an HNO value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>HNS</td>
<td>From the drop-down list box, choose an HNS value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>LMK</td>
<td>From the drop-down list box, choose an LMK value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>LOC</td>
<td>From the drop-down list box, choose a LOC value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
</tbody>
</table>
### Table 32-4 Logical Partitioning Policy Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLR</td>
<td>From the drop-down list box, choose a FLR value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>NAM</td>
<td>From the drop-down list box, choose an NAM value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
<tr>
<td>PC</td>
<td>From the drop-down list box, choose a PC value for this logical partitioning policy. You can leave the &lt;None&gt; value if you do not want to specify this field for this logical partitioning policy.</td>
</tr>
</tbody>
</table>

### Configured Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Type | After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the current logical partitioning policy for this relationship.  
**Note** Only relationships that do not specify Use Default Policy display in this pane. |
| Geolocation Policy | After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the other geolocation policy for this relationship.  
**Note** Only relationships that do not specify Use Default Policy display in this pane. |
| Other Device Type | After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the other logical partitioning policy for this relationship.  
**Note** Only relationships that do not specify Use Default Policy display in this pane. |
| Policy | After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the configured logical partitioning policy value for this relationship.  
**Note** Only relationships that do not specify Use Default Policy display in this pane. |
Table 32-4  Logical Partitioning Policy Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure Relationship to Other Geolocation Policies | From the drop-down list box, choose one of the following values to configure the relationship of this logical partitioning policy to other geolocation policies:  
  - Border—Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports.  
  - Interior—Choose this device type for devices that specify VoIP phones or internal endpoints.  
  **Note**  
  See Table 32-2 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior). |
| Geolocation Policy            | In this pane, choose the name of another geolocation policy to configure the relationship between this logical partitioning policy and that geolocation policy. |
| Other Device Type             | From the drop-down list box, choose the device type of the other geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values:  
  - Border—Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports.  
  - Interior—Choose this device type for devices that specify VoIP phones or internal endpoints.  
  **Note**  
  See Table 32-2 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior). |
| Policy                        | From the drop-down list box, choose the policy to apply between this logical partitioning policy and the geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values:  
  - Use Default Policy—Choose this value to apply the default policy that the Logical Partitioning Default Policy enterprise parameter specifies.  
  - Allow—Choose this value to specify a policy of Allow between this logical partitioning policy and the other geolocation policy.  
  - Deny—Choose this value to specify a policy of Deny between this logical partitioning policy and the other geolocation policy. |

**Additional Information**

See the “Related Topics” section on page 32-47.
Logical Partitioning Configuration Upon Upgrade From Previous Releases

During upgrade of Cisco Unified Communications Manager from a release that preceded Release 7.1(2), the following values get assigned for the entities that associate with logical partitioning configuration:

- Enable Logical Partitioning enterprise parameter specifies **False**.
- Logical Partitioning Default Policy enterprise parameter specifies **Deny**.
- Geolocation
  - No configured geolocation records exists in the geolocation table.
  - Default Geolocation enterprise parameter specifies **Unspecified**.
  - Device pools specify Geolocation value **None**.
  - Devices specify Geolocation value **Default**.
- Geolocation filter
  - No configured geolocation filter records exist in geolocation filter table.
  - Logical Partitioning Default Filter enterprise parameter specifies **None**.
  - Device pools specify Geolocation Filter value **None**.
  - Devices specify Geolocation Filter value **None**.
- Logical partitioning policy
  - No configured GeolocationPolicy records and policies exist in geolocationpolicy and geolocationpolicymatrix tables.

**Additional Information**
See the “Related Topics” section on page 32-47.

Troubleshooting Logical Partitioning

For information on troubleshooting logical partitioning, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

**Additional Information**
See the “Related Topics” section on page 32-47.

Related Topics

- Configuration Checklist for Logical Partitioning, page 32-1
- Introducing Logical Partitioning, page 32-4
- Applicability to Requirements From Indian Telecom Regulations, page 32-6
- History, page 32-7
- Overview of Logical Partitioning Architecture, page 32-8
- Logical Partitioning Use of Geolocations and Geolocation Filters, page 32-8
• Logical Partitioning Geolocation Usage for Shared Lines and Route Lists, page 32-10
• Enterprise Parameters for Logical Partitioning, page 32-10
• Logical Partitioning Policies, page 32-11
• LPPolicyManager and Policy Tree, page 32-13
• Logical Partitioning Policy Search Algorithm, page 32-15
• Policy Matching, page 32-17
• Deny Policy Handling, page 32-18
• LPSession Infrastructure and Policy Checking, page 32-18
• Logical Partitioning Handling for a Basic Call, page 32-19
• Logical Partitioning Handling of a Received Geolocation, page 32-20
• Logical Partitioning Interaction with Geolocation Conveyance Across SIP Trunks and Intercluster Trunks, page 32-19
• Logical Partitioning Feature Interactions with Midcall Geolocation Change, page 32-20
• SIP Trunk or Intercluster Trunk Configuration Requirement for Logical Partitioning, page 32-21
• System Requirements for Logical Partitioning, page 32-22
• Interactions and Limitations, page 32-22
• Interactions, page 32-22
• Call Forwarding, page 32-23
• Call Transfer, page 32-24
• Ad Hoc Conference, Join, Join Across Lines (JAL), page 32-27
• Meet-Me Conference, page 32-28
• Call Pickup, page 32-29
• Call Park and Directed Call Park, page 32-30
• Cisco Extension Mobility, page 32-31
• Cisco Unified Mobility, page 32-32
• Shared Line, page 32-33
• Barge, cBarge, and Remote Resume, page 32-34
• Route Lists and Hunt Pilots, page 32-35
• CTI Handling, page 32-36
• Limitations, page 32-37
• Configuring Logical Partitioning, page 32-39
• Geolocation Configuration, page 32-39
• Geolocation Filter Configuration, page 32-39
• Logical Partitioning Policy Configuration, page 32-40
• Logical Partitioning Policy Configuration Settings, page 32-43
• Logical Partitioning Configuration Upon Upgrade From Previous Releases, page 32-47
• Troubleshooting Logical Partitioning, page 32-47
• Device Pool Configuration,
• Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide
• CTI Route Point Configuration, Cisco Unified Communications Manager Administration Guide
• Gateway Configuration, Cisco Unified Communications Manager Administration Guide
• Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
• Trunk Configuration, Cisco Unified Communications Manager Administration Guide

Additional Cisco Documentation
• Cisco Unified Communications Manager Administration Guide
• Cisco Unified Communications Manager System Guide
• Cisco Unified Serviceability Administration Guide
• Cisco Unified Communications Manager Call Detail Records Administration Guide
• Cisco Unified Real-Time Monitoring Tool Administration Guide
• Cisco Unified Reporting Administration Guide
• Cisco Unified Communications Manager Bulk Administration Guide
• Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager
• Cisco Unified Communications Manager Security Guide
• Cisco Unified Communications Manager Assistant User Guide
Malicious Call Identification

This chapter provides the following information about the Malicious Call Identification feature:

- Configuration Checklist for Malicious Call ID, page 33-1
- Introducing Malicious Call Identification, page 33-2
- System Requirements for Malicious Call ID, page 33-3
- Devices That Support Malicious Call Identification, page 33-4
- Interactions and Restrictions, page 33-4
- Installing Malicious Call ID, page 33-6
- Configuring Malicious Call ID, page 33-6
- Troubleshooting Malicious Call ID, page 33-10
- Related Topics, page 33-11

Configuration Checklist for Malicious Call ID

The malicious call identification (MCID) feature allows a user to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.

Malicious call identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature button while the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.
Table 33-1 provides a checklist for configuring malicious call identification. For additional information on malicious call identification, see the “Introducing Malicious Call Identification” section on page 33-2 and the “Related Topics” section on page 33-11.

### Table 33-1 MCID Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure the CDR service parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure the alarm.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>If users will access MCID by using a softkey, configure a softkey template with the Toggle Malicious Call Trace (MCID) softkey.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Cisco Unified IP Phones 8900 and 9900 series support MCID with feature button only.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assign the MCID softkey template to an IP phone.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>If users will access MCID by using a feature button, configure a phone button template with the Malicious Call Identification feature.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Assign the MCID phone button template to an IP phone.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Notify users that the Malicious Call Identification feature is available.</td>
</tr>
</tbody>
</table>

### Introducing Malicious Call Identification

The Malicious Call Identification (MCID) supplementary service allows you to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.
Malicious Call Identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature code while the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.

The system supports the MCID service, which is an ISDN PRI service, when it is using PRI connections to the PSTN. The MCID service includes two components:

1. **MCID-O**—An originating component that invokes the feature upon the user request and sends the invocation request to the connected network.
2. **MCID-T**—A terminating component that receives the invocation request from the connected network and responds with a success or failure message that indicates whether the service can be performed.

**Note** Cisco Unified Communications Manager supports only the originating component.

### Using the Malicious Call ID Feature with Cisco Unified Communications Manager

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified Communications Manager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

When the MCID feature is used, the following actions take place:

1. The user receives a threatening call and presses Malicious Call (or enters the feature code *39).
2. Cisco Unified Communications Manager sends the user a confirmation tone if the device can play a tone—and a text message on a phone that has a display—to acknowledge receiving the MCID notification.
3. Cisco Unified Communications Manager updates the CDR for the call with an indication that the call is registered as a malicious call.
4. Cisco Unified Communications Manager generates the alarm and local syslogs entry that has the event information.
5. Cisco Unified Communications Manager sends an MCID invocation through the facility message to the connected network. The facility information element (IE) encodes the MCID invocation.
6. After receiving this notification, the PSTN or other connected network can take actions, such as providing legal authorities with the call information.

### System Requirements for Malicious Call ID

Malicious Call ID service requires Cisco Unified Communications Manager 5.0 or later to operate. The following gateways and connections support MCID service:

- PRI gateways that use the MGCP PRI backhaul interface for T1 (NI2) and E1 (ETSI) connections.
- H.323 trunks and gateways

The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

To determine which IP Phones support the MCID feature, see the “Devices That Support Malicious Call Identification” section on page 33-4.

Devices That Support Malicious Call Identification

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support MCID. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click System Reports in the navigation bar.

3. In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.

4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

5. To generate a report of all IP Phones that support MCID, choose these settings from the respective drop-down list boxes and click the Submit button:
   - Product: All
   - Feature: Malicious Call Identification

   The List Features pane displays a list of all devices that support the MCID feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

   For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Interactions and Restrictions

The following sections describe the interactions and restrictions for Malicious Call Identification.

- Interactions, page 33-5
- Restrictions, page 33-6
Interactions

The following sections describe how Malicious Call Identification interacts with Cisco Unified Communications Manager applications and call processing:

- Conference Calls, page 33-5
- Extension Mobility, page 33-5
- Call Detail Records, page 33-5
- Alarms, page 33-5

Conference Calls

When a user is connected to a conference, the user can use the MCID feature to flag the call as a malicious call. Cisco Unified Communications Manager sends the MCID indication to the user, generates the alarm, and updates the CDR. However, Cisco Unified Communications Manager does not send an MCID invoke message to the connected network that might be involved in the conference.

Extension Mobility

Extension mobility users can have the MCID softkey as part of their user device profile and can use this feature when they are logged on to a phone.

Call Detail Records

To track malicious calls by using CDR, you must set the CDR Enabled Flag to True in the Cisco CallManager service parameter. When the MCID feature is used during a call, the CDR for the call contains “CallFlag=MALICIOUS” in the Comment field.

Alarms

To record alarms for the MCID feature in the Local Syslogs, you must configure alarms in Cisco Unified Serviceability. Under Local Syslogs, enable alarms for the “Informational” alarm event level.

When the MCID feature is used during a call, the system logs an SDL trace and a Cisco Unified Communications Manager trace in alarms. You can view the Alarm Event Log by using Cisco Unified Serviceability. The traces provide the following information:

- Date and time
- Type of event: Information
- Information: Malicious Call Identification feature gets invoked in Cisco Unified Communications Manager
- Called Party Number
- Called Device Name
- Called Display Name
- Calling Party Number
- Calling Device Name
- Calling Display Name
• Application ID  
• Cluster ID  
• Node ID  

See the *Cisco Unified Serviceability Administration Guide* for more information about alarms and traces.

**Restrictions**

The following restrictions apply to Malicious Call Identification:

• Cisco Unified Communications Manager supports only the malicious call identification originating function (MCID-O). Cisco Unified Communications Manager does not support the malicious call identification terminating function (MCID-T). If Cisco Unified Communications Manager receives a notification from the network of a malicious call identification, Cisco Unified Communications Manager ignores the notification.

• MCID does not work across intercluster trunks because Cisco Unified Communications Manager does not support the MCID-T function.

• Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.

• MCID does not work over QSIG trunks because MCID is not a QSIG standard.

• The Cisco VG248 Analog Phone Gateway does not support MCID.

• Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.

• MCID does not support SIP trunks.

See the “Configuring Malicious Call ID” section on page 33-6 for configuration details.

**Installing Malicious Call ID**

Malicious Call Identification, which is a system feature, comes standard with Cisco Unified Communications Manager software. MCID does not require special installation or activation.

**Configuring Malicious Call ID**

This section contains the following information:

• Setting the Service Parameter for Malicious Call ID, page 33-7  
• Configuring Alarms for Malicious Call ID, page 33-7  
• Adding a Softkey Template for Malicious Call ID, page 33-8  
• Giving the Malicious Call Identification Feature to Users, page 33-8  
• Removing the Malicious Call Identification Feature from a User, page 33-9  
• Adding a Phone Button Template for Malicious Call ID, page 33-9  
• Giving the Malicious Call Identification Feature to Users, page 33-10
Tip
Before you configure Malicious Call Identification, review the “Configuration Checklist for Malicious Call ID” section on page 33-1.

Setting the Service Parameter for Malicious Call ID

To enable Cisco Unified Communications Manager to flag a CDR with the MCID indicator, you must enable the CDR flag. Use the following procedure in Cisco Unified Communications Manager Administration to enable CDR.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose System > Service Parameters.
Step 2 Choose the Cisco Unified Communications Manager server name.
Step 3 In the Service field, choose Cisco CallManager. The Service Parameters Configuration window displays.
Step 4 In the System area, set the CDR Enabled Flag field to True if it is not already enabled.
Step 5 If you need to make the change, click Save.

Configuring Alarms for Malicious Call ID

To ensure that the MCID alarm information appears in the Local Syslogs, you need to enable the alarm event level. Use Cisco Unified Serviceability and the following procedure to activate alarms for MCID.

Procedure

Step 1 From the Navigation drop-down list box, choose Cisco Unified Serviceability and click Go. Cisco Unified Serviceability displays.
Step 2 Choose Alarm > Configuration. The Alarm Configuration window displays.
Step 3 From the servers list, choose the Cisco Unified Communications Manager server.
Step 4 In the Configured Services list box, choose Cisco CallManager. The Alarm Configuration window updates with configuration fields.
Step 5 Under Local Syslogs, in the Alarm Event Level drop-down list, choose Informational.
Step 6 Under Local Syslogs, check the Enable Alarm check box.
Step 7 If you want to enable the alarm for all nodes in the cluster, check the Apply to All Nodes check box.
Step 8 To turn on the informational alarm, click Update.

Additional Information
See the “Related Topics” section on page 33-11.
Adding a Softkey Template for Malicious Call ID

Use this procedure in Cisco Unified Communications Manager Administration to add the Malicious Call softkey to a template.

Procedure

Step 1. From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Softkey Template. The Find and List Softkey Templates window displays.

Step 2. Click the Add New button. The Softkey Template Configuration window displays.

Step 3. In the Create a softkey template based on field, choose Standard User.

Step 4. Click Copy. The Softkey Template Configuration window refreshes with new fields.

Step 5. In the Softkey Template Name field, enter a name that indicates that this is an MCID softkey template.

Step 6. In the Description field, enter a description that indicates that this is an MCID softkey template.

Step 7. Click Save. The Softkey Template Configuration window refreshes with additional configuration fields.

Step 8. Click the Go button that is next to the Configure Softkey Layout related links box. The Softkey Layout Configuration window displays.

Step 9. In the Select a call state to configure field, choose Connected. The list of Unselected Softkeys changes to display the available softkeys for this call state.

Step 10. In the Unselected Softkeys list, choose Toggle Malicious Call Trace (MCID).

Step 11. To move the softkey to the Selected keys list, click the right arrow.

Step 12. To ensure that the softkey template is configured, click Save.

Additional Information

See the “Related Topics” section on page 33-11.

Giving the Malicious Call Identification Feature to Users

To provide the Malicious Call Identification feature for users, you assign the MCID softkey template to their IP phone.

Note

For users who do not have phones that can use a softkey, give them the feature code information and instructions on how to invoke the feature.

Procedure

Step 1. Choose Device > Phone. The Find and List Phones window displays.

Step 2. To locate the phone configuration, enter appropriate phone search information; click Find.

Step 3. Choose the phone that you want to update.

Step 4. Locate the Softkey Template field and choose the MCID softkey template that you created from the drop-down list.
Step 5  To save the changes in the database, click **Save**.
Step 6  To activate the changes on the phone, click **Reset**.
Step 7  Notify the user that the Malicious Call Identification feature is available.

**Additional Information**
See the “Related Topics” section on page 33-11.

### Removing the Malicious Call Identification Feature from a User

To remove the Malicious Call Identification feature from users, you assign another softkey template to their IP phone.

**Procedure**

- **Step 1**  Choose **Device > Phone**. The Find and List Phones window displays.
- **Step 2**  To locate the phone configuration, enter appropriate phone search information and click **Find**.
- **Step 3**  Choose the phone that you want to update.
- **Step 4**  Locate the Softkey Template field and choose a soft key template without MCID from the drop-down list.
- **Step 5**  To save the changes in the database, click **Save**.
- **Step 6**  To activate the changes on the phone, click **Reset**.
- **Step 7**  Notify the user that the Malicious Call Identification feature is no longer available.

**Additional Information**
See the “Related Topics” section on page 33-11.

### Adding a Phone Button Template for Malicious Call ID

Use this procedure in Cisco Unified Communications Manager Administration to add the Malicious Call button to a phone button template.

**Procedure**

- **Step 1**  From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Phone Button Template**. The Find and List Phone Button Templates window displays.
- **Step 2**  Click the **Add New** button. The Phone Button Template Configuration window displays.
- **Step 3**  In the Phone Button Template drop-down list box, choose the phone button template for the IP phone.
- **Step 4**  Click **Copy**. The Phone Button Template Configuration window displays.
- **Step 5**  In the Button Template Name field, enter a name that indicates that this is an MCID phone button template.
- **Step 6**  Click **Save**. The Phone Button Template Configuration window redisplays with new fields.
Chapter 33  Malicious Call Identification

Step 7  Choose a line button that you want the MCID feature assigned; for example button 3.
Step 8  From the drop-down list box for the line button you chose, choose Malicious Call Identification.
Step 9  Click Save. The Phone Button Template Configuration window refreshes.

Additional Information
See the “Related Topics” section on page 33-11.

Giving the Malicious Call Identification Feature to Users

To provide the Malicious Call Identification feature for users, you assign the MCID phone button template to their IP phone.

Procedure

Step 1  Choose Device > Phone. The Find and List Phones window displays.
Step 2  To locate the phone configuration, enter appropriate phone search information; click Find.
Step 3  Choose the phone that you want to update.
Step 4  Locate the Phone Button Template field and choose the MCID phone button template that you created from the drop-down list.
Step 5  To save the changes in the database, click Save.
Step 6  To activate the changes on the phone, click Reset.
Step 7  Notify the user that the Malicious Call Identification feature is available.

Additional Information
See the “Related Topics” section on page 33-11.

Troubleshooting Malicious Call ID

To assist with tracking and troubleshooting the Malicious Call ID feature, the system makes Cisco Unified Communications Manager SDL traces and alarms available.

For information about using these traces and alarms, see the Cisco Unified Serviceability Administration Guide.

Additional Information
See the “Related Topics” section on page 33-11.
Related Topics

- Configuration Checklist for Malicious Call ID, page 33-1
- Introducing Malicious Call Identification, page 33-2
- System Requirements for Malicious Call ID, page 33-3
- Interactions and Restrictions, page 33-4
- Installing Malicious Call ID, page 33-6
- Configuring Malicious Call ID, page 33-6
- Troubleshooting Malicious Call ID, page 33-10
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- Configuration Checklist for Malicious Call ID, page 33-1
- Setting the Service Parameter for Malicious Call ID, page 33-7
- Adding a Softkey Template for Malicious Call ID, page 33-8
- Configuring Alarms for Malicious Call ID, page 33-7
- Giving the Malicious Call Identification Feature to Users, page 33-8
- Removing the Malicious Call Identification Feature from a User, page 33-9

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone user documentation and release notes (all models)
Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The Silent Call Monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer; neither the agent nor the customer can hear the supervisor voice.

The Call Recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.

Cisco Unified Communications Manager supports the Silent Call Monitoring and Call Recording features only within a single cluster.

The Silent Monitoring and Call Recording features specify generic features in Cisco Unified Communications Manager. Cisco makes these features available to any deployment or installation where monitoring- and recording-enabled applications are available. Descriptions in this document use terms such as supervisor, agent, and customer to see the parties that participate in call monitoring and recording sessions.

The following topics discuss silent call monitoring and call recording:

- Configuration Checklist for Monitoring and Recording, page 34-1
- Introducing Monitoring and Recording, page 34-2
- System Requirements for Monitoring and Recording, page 34-59
- Interactions and Limitations, page 34-60
- Configuring Monitoring and Recording, page 34-63
- Related Topics, page 34-75

**Configuration Checklist for Monitoring and Recording**

Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The silent call monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer; neither the agent nor the customer can hear the supervisor voice. The call recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.
Introducing Monitoring and Recording

The steps in Table 34-1 summarize the actions that are needed to configure monitoring and recording. For more information on monitoring and recording, see the “Introducing Monitoring and Recording” section on page 34-2 and the “Related Topics” section on page 34-75.

Table 34-1 Monitoring and Recording Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Turn on IP phone BIB to allow monitoring or recording.</td>
<td>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add user for monitoring or recording application.</td>
<td>Application User Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add user to groups that allow monitoring and recording.</td>
<td>Application User Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 4</td>
<td>Optional. Configure tones for monitoring or recording.</td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure DN for a monitoring calling search space.</td>
<td>Directory Number Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enable recording for a line appearance.</td>
<td>Directory Number Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 7</td>
<td>Create a recording profile.</td>
<td>Recording Profile Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 8</td>
<td>Optional. Create a SIP profile for recording.</td>
<td>SIP Profile Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 9</td>
<td>Create a SIP trunk that points to the recorder.</td>
<td>Trunk Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 10</td>
<td>Create a route pattern for the recorder.</td>
<td>Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 11</td>
<td>Configure recorder redundancy.</td>
<td>Trunk Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>

Introducing Monitoring and Recording

The following topics introduce call monitoring and call recording:

- Terminology for Call Monitoring and Call Recording, page 34-3
- Call Recording Overview, page 34-3
- Monitoring and Recording Architecture, page 34-4
- Devices That Support Call Monitoring and Call Recording, page 34-6
- Introduction to Call Monitoring, page 34-8
- Introduction to Call Recording, page 34-16
- Call Characteristics of Monitoring and Recording Calls, page 34-55
Terminology for Call Monitoring and Call Recording

This document uses the following terms to discuss call monitoring and call recording:

- **Agent**—A call center employee who takes calls from customers.
- **Call monitoring**—A Cisco Unified Communications Manager feature that allows the monitoring party to listen to or participate in a conversation between or among other parties.
- **Call recording**—A Cisco Unified Communications Manager feature that allows a recording device to record a conversation between or among other parties.
- **Customer**—In this document, refers to a caller that calls into a call center.
- **Local stream**—The media stream from agent to customer.
- **Recorder**—A recording party.
- **Recording application**—A recording-enabled application that invokes a recording session.
- **Remote stream**—The media stream from customer to agent.
- **Supervisor**—The supervisor of agents. A supervisor can monitor the call between an agent and a customer.
- **Supervisor desktop application**—A monitoring-enabled application that gets used to invoke a monitoring session.
- **Silent monitoring**—A mode of call monitoring. The Cisco Unified Communications Manager silent monitoring feature allows a monitoring party (a supervisor) to listen to a conversation between a near-end party (an agent) and a far-end party (a customer); neither the near-end party nor the far-end party hears the monitoring party voice.

Call Recording Overview

Call recording specifies a call center ability to archive the agent conversations. The following types of call recording exist:

- **Total Recording**—All calls of an agent automatically get recorded.
- **Selective Recording**—Only a percentage of calls of agents get recorded.
Figure 34-1 illustrates call recording.

**Figure 34-1 Call Recording Overview**

Call monitoring and call recording represent essential features in call centers. Environments other than the traditional call center sometimes use call monitoring and call recording to meet regulatory or quality requirements that an enterprise faces.

Various architectures can accomplish call monitoring and call recording. Cisco Unified Communications Manager uses an IP phone-based architecture to provide call monitoring and call recording. The IP phone-based architecture exhibits the following methods:

- **IP phone-based call monitoring**—The agent phone mixes the agent voice with the customer voice and sends the mix of both voices to the supervisor phone.
- **IP phone-based call recording**—The agent phone forks two streams to the recorder: one recording stream comprises the agent voice and the other recording stream comprises the customer voice.

See the “SIP Header Enhancements for Call Recording” section on page 34-18 for a discussion of the SIP header enhancements that were made in Release 8.5(1).
Figure 34-2 illustrates the IP phone-based architecture for monitoring and recording. In the figure, the blue lines indicate the agent voice stream, the red lines indicate the customer voice stream, and the green line indicates the mix of customer and agent voice streams that gets sent to the supervisor.

Figure 34-2   IP Phone-Based Architecture for Monitoring and Recording
Figure 34-3 illustrates the streaming through the agent IP phone. In the figure, the blue lines indicate the agent voice stream, the red lines indicate the customer voice stream, and the green line indicates the mix of customer and agent voice streams that gets sent to the supervisor.

The call monitoring and call recording features impose requirements upon the following areas:

- CTI/JTAPI/TSP
- Call processing
- Cisco Unified Communications Manager Administration
- Cisco Unified Communications Manager database
- IP Phone Firmware

**Devices That Support Call Monitoring and Call Recording**

This section lists and describes the various devices that support call monitoring and call recording.

**Agent Devices**

Agent devices must be able to mix media for monitoring and to fork media for recording.

The list of devices that support the monitoring and recording features varies per version and device pack. Use the Cisco Unified Reporting application to generate a complete list of devices that support monitoring and recording for a particular release and device pack. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   
   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
Introducing Monitoring and Recording

2. Click **System Reports** in the navigation bar.

3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all devices that support monitoring, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Monitor

   The List Features pane displays a list of all devices that support the monitoring feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

6. To generate a report of all devices that support recording, choose these settings from the respective drop-down list boxes and click the **Submit** button:
   - **Product**: All
   - **Feature**: Record

   The List Features pane displays a list of all devices that support the recording feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the *Cisco Unified Reporting Administration Guide*, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

**Supervisor Devices**

Supervisor devices must be able to receive one-way media.

**Recorders**

Recorders must interface with Cisco Unified Communications Manager SIP trunk to receive recording calls.

Nice/Witness Recorders have been tested; Verint and other third-party vendors manufacture suitable recorders.
**Introduction to Call Monitoring**

With silent call monitoring, the supervisor can listen in on an agent call for quality control and performance evaluation. By default, the agent is not aware of the monitoring session. In IP phone-based silent call monitoring, the monitoring stream comprises a mix of the customer voice and the agent voice. Only an application can trigger a monitoring session. **Figure 34-4** shows the flow during a typical monitoring session.

**Figure 34-4  Silent Call Monitoring Session Flow**

Only an application can invoke monitoring through the JTAPI or TAPI interfaces of Cisco Unified Communications Manager. Monitoring exhibits these characteristics:

- Because monitoring is call based, the monitoring target specifies a specific call on a line appearance of an agent.
- A start monitoring request from the application triggers the supervisor phone to go off hook automatically and make a monitoring call to the agent.
- The agent phone automatically accepts the monitoring call. The monitoring call does not get presented to the agent.

The Cisco Unified Communications Manager user interface and an application control authentication and authorization for monitoring. The following requirements apply:

- The application user needs to be a member of the Standard CTI Allow Call Monitoring user group.
- The agent device needs to be in the application user CTI control list.

**Invocation of a Silent Monitoring Session**

A supervisor can initiate a silent monitoring session by using a desktop application after the agent answers a call.
Figure 34-5 illustrates a silent monitoring session.

When the supervisor initiates a monitoring session, the following steps take place:

1. The customer calls into the call center. The call gets routed to the agent.
2. The agent answers the call. A two-way media stream gets set up between the agent IP phone and the customer.
3. The supervisor selects the agent from his desktop application, and then clicks Monitoring.
4. The supervisor phone automatically goes off hook.
5. The supervisor phone makes a monitoring call to the agent.
6. The built-in bridge (BIB) of the agent phone automatically accepts the monitoring call. The agent phone starts to mix media of the agent voice and the customer voice and sends the mix to the supervisor phone.

Be aware that the supervisor must be located in the same cluster as the agent to start the silent monitoring session. However, the supervisor can transfer the monitoring call anywhere after the monitoring call is initiated.

The supervisor can terminate the monitoring call anytime after the call starts, either through the application or simply by hanging up.

The supervisor can put the monitoring call on hold (no MOH gets inserted) and resume the monitoring call from the same or a different device.
Supervisor Transfers the Monitoring Call

Figure 34-6 illustrates the supervisor transfer of a monitoring call.

During a monitoring call, the supervisor transfers the monitoring call, and the following steps take place:

1. Supervisor 1 presses the Transfer softkey and dials the phone number of supervisor 2.
2. Supervisor 2 answers the call.
3. Supervisor 1 completes the transfer by pressing the Transfer softkey again.
4. The monitoring call transfers to supervisor 2. Supervisor 2 starts to receive the mix of the agent voice and the customer voice.

Agent Cannot Control a Monitoring Call

The agent does not have direct control over the monitoring call; however, the agent action on the primary call causes a corresponding action for the monitoring call.

When an agent puts the customer on hold, Cisco Unified Communications Manager also puts the monitoring call on hold, but no MOH gets inserted. When the agent hangs up the call with the customer, the monitoring call terminates.
Figure 34-7 illustrates the scenario where the agent puts the customer on hold while the supervisor is monitoring the agent.

**Figure 34-7  Agent Does Not Control the Monitoring Call**

While an agent is being monitored, the agent puts the customer on hold, and the following steps take place:

1. The agent puts the customer on hold. MOH gets inserted and played to the customer.
2. Cisco Unified Communications Manager automatically puts the supervisor on hold. No MOH gets inserted to the supervisor.
Multiple Monitoring Sessions

Figure 34-8 illustrates the call flows during multiple monitoring sessions.

During multiple monitoring sessions, the following steps take place:

1. Customer 2 calls the agent while the agent is in a call with customer 1 and supervisor is monitoring the agent call with customer 1.
2. The agent puts customer 1 on hold; MOH gets inserted to customer 1.
3. Cisco Unified Communications Manager puts the supervisor on hold. No MOH gets inserted to the supervisor.
4. The agent answers customer 2 call.
5. The supervisor initiates a second monitoring request for the agent call with customer 2.
6. The supervisor phone automatically puts the first monitoring call on hold.
7. The supervisor phone goes off hook and makes the second monitoring call to the agent.
8. The agent IP phone (BIB of the agent IP phone) automatically accepts the monitoring call. The mix of agent voice and customer 2 voice gets sent to the supervisor phone.

Barging or Monitoring an Agent Call

If the agent call is being monitored, the barge-in call from a shared line fails.
If the agent call is barged in, the monitoring request gets rejected with a No resource error.
Monitoring an Agent in a Conference

An agent in a call center sometime needs to bring in another party into the conversation with the customer.

Figure 34-9 illustrates a case where agent1 starts an ad hoc conference to include agent2 in the conversation with the customer. The supervisor for agent1 monitors the original call with the customer.

During the setting-up process, the media of the monitoring call disconnect briefly. After the conference completes, the supervisor can hear all the parties that are included in the conference.

Figure 34-9 Monitoring an Agent in a Conference
Agent Conferences in the Supervisor

The agent may create a conference with the supervisor while that supervisor is monitoring that agent. The supervisor must put the monitoring call on hold before joining the conference. Figure 34-10 illustrates this scenario.

Figure 34-10 shows the final connection when the supervisor puts the monitoring call on hold and joins the conference. The monitoring session remains in the hold state while the supervisor participates in the conference. After the supervisor leaves the conference, he can then resume the monitoring session.
Supervisor Conferences in Another Supervisor

A supervisor can conference another supervisor for the monitoring session.
Supervisors can hear and talk to each other, and both can hear the conversation of the agent with the customer.

Figure 34-11 illustrates this scenario.

Figure 34-11  Supervisor Conferences in Another Supervisor

In the example shown in Figure 34-11, supervisor 1, who started a monitoring call to the agent, conferences in supervisor 2 to the monitoring call. The customer and agent can still hear each other and are not aware of any of the monitoring supervisors. Both supervisor 1 and the supervisor 2 can hear the conversation of the agent with the customer. The two supervisors can hear each other.

Whisper Coaching

Whisper coaching is an enhancement to silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature provides applications the ability to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

To enable Whisper Coaching in the Cisco Unified Communications Manager Administration application, choose Device > Phone, locate the Cisco Unified IP Phone that you want to configure.
Scroll to the Device Information Layout pane and set Built-in Bridge to On or Default. If Built-in Bridge is set to Default, in the Cisco Unified Communications Manager Administration application, choose System > Service Parameter and select the appropriate Server and Service. Scroll to the Clusterwide Parameters (Device - Phone) pane and set Built-in Bridge Enable to On.
Introduction to Call Recording

In IP phone-based call recording, recording streams get forked from agent IP phone to the recorder: The agent voice and the customer voice get sent separately.

The administrator configures the recorder in Cisco Unified Communications Manager as a SIP trunk device.

This section covers the following general topics that apply to call recording:

- Call Recording Session Flow, page 34-17
- Call Recording Modes, page 34-17
- SIP Header Enhancements for Call Recording, page 34-18
- Recorder as SIP Trunk Device, page 34-18

This section provides detailed call flows and detailed explanations of the following use cases when an agent device is configured for automatic call recording:

- Automatic Call Recording, page 34-19
- Local Cluster Far-End Party Hold/Resume, page 34-21
- Far-End Party Transfers Call to Another Far-End Party in Local Cluster, page 34-23
- Near-End Party Transfers Call to Another Near-End Party in Local Cluster, page 34-25
- Far-End Party Transfers Call to CFNA-Enabled Party, page 34-28
- Far-End Party in Local Cluster Creates Conference, page 34-30
- Near-End Party in Local Cluster Creates Conference, page 34-32
- Far-End Party in Remote Cluster Transfers Call to Another Party in Remote Cluster, page 34-34
- Far-End Party in Remote Cluster Blind-Transfers Call to Remote-Cluster Party That Has CFNA Configured, page 34-36
- Far-End Party in Remote PBX Transfers Call to Phone in Local Cluster, page 34-38
- Remote PBX Far-End Party Transfers Call to Local Phone With Path Replacement, page 34-40
- Far-End Party Transfers Call Across DMS Gateway, page 34-42
- Desktop Pickup of Mobile Phone Call, page 34-44
- Far-End Party Sends Call to Mobile Phone for Mobile Phone Pickup, page 34-46
- Far-End Party in Remote Cluster Creates Conference, page 34-47

This section discusses the following additional call-recording use cases:

- Application-Invoked Recording, page 34-49
- Recording Calls Do Not Survive Agent Hold, page 34-50
- Recording a Barged Call, page 34-52
- Recording an Agent Conference, page 34-52
- Simultaneous Monitoring and Recording, page 34-54
### Call Recording Session Flow

Figure 34-12 illustrates IP phone-based call recording session flow.

**Figure 34-12  IP Phone-Based Call Recording**

![Call Recording Diagram]

### Call Recording Modes

The following modes of call recording exist:

- **Automatic recording**—In automatic recording, the recording session automatically establishes when the agent call connects.
- **Application-invoked recording**—In application-invoked recording, the application invokes the recording session for an active call through TAPI or JTAPI API.
- **Device-invoked call recording**—Device-invoked call recording applies only to a specific External Call Control call that is known as a *chaperone call*. A softkey on the chaperone phone invokes the recording session. The External Call Control feature controls this type of call recording. See the “External Call Control” chapter for details. (The chaperone call involves a policy server; this softkey-invoked call recording type is not available for general use.)

#### Note

In all call recording modes, the agent call must be active before call recording takes place.

The administrator configures the recording option and recording profile on the agent line appearance. By default, the recording option specifies Call Recording Disabled.
When the recording option is set to either Automatic Call Recording Enabled or Application Invoked Call Recording Enabled, the line appearance can be associated with a recording profile. The recording profile specifies the following parameters: Recording Calling Search Space and Recording Destination Address.

When automatic recording is enabled, the application recording requests get rejected.

**SIP Header Enhancements for Call Recording**

Release 8.5(1) of Cisco Unified Communications Manager introduces enhancements to the SIP headers that are used in the SIP messages that are sent to the recorder when call recording calls are made. These enhancements entail the following changes:

- Cisco Unified Communications Manager sends both the agent (near-end) and customer (far-end) call information to the recorder via SIP messages. Messages travel through the SIP trunk. (Prior to this enhancement, only the near-end information was sent via SIP messages; retrieval of the far-end information required a CTI connection to Cisco Unified Communications Manager.)

- The enhancement increases scalability: the recorder no longer requires a CTI connection to Cisco Unified Communications Manager to obtain far-end call information from Cisco Unified Communications Manager.

- The enhancement supports automatic recording through use of the Open Recording Architecture (ORA) Cisco Zephyr recorder. Thus, a complete call-recording solution that uses only Cisco products is now available. The Cisco Zephyr recorder provides a basic and powerful recording capability and does not rely on CTI to obtain the far-end information.

The From header contains the near-end call info. The near-end call information contains refci or the call ID of the near-end party, near-end device name, near-end directory number or address.

With the SIP header enhancement, the far-end call information gets added to the INVITE message From header. The far-end call information contains farendRefCI or the call ID of the far-end party, far-end device name, and far-end directory number.

Previously, Cisco Unified Communications Manager only sent a SIP INVITE message to a recorder. Now, when the far-end call info changes due to feature interaction, Cisco Unified Communications Manager sends a SIP UPDATE message to the recorder.

The From header also includes an *isfocus* indicator, which indicates that an agent is in a conference call.

Examples of the previous INVITE message and the new INVITE and UPDATE messages follow.

**Previous From Header in SIP INVITE Message**

```
From: <sip:3005@10.89.81.56;x-nearend;x-refci=25471846;x-nearenddevice=SEP001B535CDC62 >;
```

**New From Header in SIP INVITE and UPDATE Messages**

```
From: 
<sip:3005@10.89.81.56;x-nearend;x-refci=25471846;x-nearenddevice=SEP001B535CDC62;x-farendrefci=25471847;x-farenddevice=CFB_2;x-farendaddr=b097865452;isfocus>;
```

In the new From header, the **text in bold** indicates the new information that the SIP header enhancement includes.

**Recorder as SIP Trunk Device**

The SIP trunk points directly to the recorder. Many recorders (such as those from Witness and Nice) consist of proxy, logger or storage and database.
The recorder accepts recording calls from Cisco Unified Communications Manager in SIP. A directory number gets assigned to the recorder; a route pattern gets configured for the SIP trunk.

**Automatic Call Recording**

In automatic call recording, after an agent call becomes active, two server calls get made to the built-in bridge (BIB) of the agent phone. The agent phone automatically answers. Two server calls then get redirected to the recorder. Figure 34-13 illustrates automatic call recording.

![Figure 34-13 Automatic Call Recording](image)

In this example of an automatic call recording session, the following entities participate:

- The customer call originates from DN 1000 device A.
- The agent receives the call at DN 2000 device B.

During an automatic call recording session, the following steps take place:

1. A customer, party A (the far-end party) with DN 1000, calls into the call center.
2. The call routes to the agent, who is party B with DN 2000. The agent answers the call. The agent IP phone starts to exchange media streams with the customer.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the agent IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the agent IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.
In previous releases, the INVITE message contained only near-end information, but customer information was unknown. A CTI connection to Cisco Unified Communications Manager was required to obtain the customer information.

Be aware that the two INVITE messages for the two separate voice streams contain the same near-end and far-end call information. The only difference in the two From headers is the first x- parameter, which indicates whether the call is for the near-end voice stream or for the far-end voice stream. x-nearend indicates the near-end voice stream. x-farend indicates the far-end voice stream.

The INVITE message that is explained here (another INVITE message gets sent) contains the agent recording call.

Note the header information of the INVITE messages from step 5 and step 6. The SIP header enhancement feature adds the information in **bold text** to the INVITE message headers.

**Step 5 INVITE Message Header Information**

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1

**Step 6 INVITE Message Header Information**

From:
<sip:2000@ucm1;x-farend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag2

In both message headers,

- **x-farendrefci** specifies the far-end (customer) call leg caller ID.
- **x-farenddevice** specifies the far-end device name.
- **x-farendaddr** specifies the far-end DN.
Local Cluster Far-End Party Hold/Resume

In this use case for automatic call recording, the far-end party that belongs to the local cluster places the call on hold and resumes the call from a different device. Figure 34-14 illustrates this use case.

**Figure 34-14 Far-End Party in Local Cluster Holds and Resumes Call From Different Device**

In this use case, the following entities participate:

- The customer call originates from DN 1000 device A.
- The agent receives the call at DN 2000 device B.
- After placing the call on hold, the customer resumes the call from DN 1000 device A'.

During an automatic call recording session that involves a customer (far-end party) in the local cluster that places the call on hold then resumes the call from a different device, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the agent IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the agent IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.

6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.

7. Party A (far-end party = customer in local cluster) places the call on hold.

8. Party A (far-end party = customer in local cluster) resumes the held call from device A’ (a different device with same DN). Upon call resumption, party B is now connected to the new far-end party A’. The far-end call information has changed.

9. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

10. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Insertion of MOH when the far-end party places the call on hold does not cause a change in the far-end party.
- When another device that shares the line resumes the call, a SIP UPDATE message gets sent to the recorder with the new far-end party device name.

The UPDATE message that is explained here contains the agent (near-end) recording call. The other UPDATE for the customer (far-end) recording call contains the same information for the x-farend.

Note the header information of the INVITE message from step 5 and the UPDATE message from step 9. The SIP header enhancement feature adds the information in **bold text** to the message headers.

**Step 5 INVITE Message Header Information**

From:

```
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```

**Step 9 UPDATE Message Header Information**

From:

```
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA';x-farendaddr=1000>;tag=fromtag1
```
Far-End Party Transfers Call to Another Far-End Party in Local Cluster

In this use case for automatic call recording, the far-end party in the local cluster transfers the call to another far-end party in the same local cluster. Figure 34-15 illustrates this use case.

**Figure 34-15  Far-End Party in Local Cluster Transfers Call to Another Far-End Party in Local Cluster**

![Diagram](image)

In this use case, the following entities participate:
- The customer call originates from DN 1000 device A in the local cluster.
- The agent receives the call at DN 2000 device B.
- The customer transfers the call to DN 1100 device C in the same local cluster.

During an automatic call recording session that involves a customer (far-end party) in the local cluster that places the call to the agent and then later transfers the call to another far-end party in the local cluster, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the agent IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the agent IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.
7. Party A (far-end party = customer in local cluster) initiates a consultation transfer of the call to another party, party C at DN 1100, in the local cluster.
8. Party C answers the transferred call.
9. Party A completes the transfer.
10. Because party B is now connected to a new far-end party, party C, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

11. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- After first press of the Transfer key, because no change in the far-end party information occurs, Cisco Unified Communications Manager does not update the recorder.
- After the second press of the Transfer key, Cisco Unified Communications Manager sends the SIP UPDATE message to the recorder with updated far-end party information.

Note the following particularities of call processing that apply in this use case:

1. Insertion of MOH when the far-end party places the call on hold does not cause a change in the far-end party.
2. When another device that shares the line resumes the call, a SIP UPDATE message gets sent to the recorder with the new far-end party device name.

Note the header information of the INVITE message from step 5 and the UPDATE message from step 10. The SIP header enhancement feature adds the information in bold text to the message headers.

**Step 5 INVITE Message Header Information**

```
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```

**Step 10 UPDATE Message Header Information**

```
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci4;x-farenddevice=deviceC;x-farendaddr=1100>;tag=fromtag1
```

When you compare the INVITE message header in step 5 with the UPDATE message header in step 10, notice that the far-end values (farendrefci, farenddevice, and farendaddr) all change because of the transfer.
Near-End Party Transfers Call to Another Near-End Party in Local Cluster

In this use case for automatic call recording, the near-end party transfers a call to another near-end party in the local cluster. Figure 34-16 illustrates this use case.

Figure 34-16 Near-End Party Transfers Call to Another Near-End Party in Local Cluster

In this use case, the following entities participate:

- The customer call originates from DN 1000 device A.
- The agent receives the call at DN 2000 device B.
- The agent transfers the call to DN 2001 device D.

During an automatic call recording session where the agent on the call transfers the call to another party in the same local cluster, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B (near-end party = agent in local cluster) answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the agent IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the agent IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.
7. Party B initiates the consultation transfer. This action implicitly places the call on hold.
8. Cisco Unified Communications Manager terminates recording of the agent voice by sending a BYE message to the recorder through a SIP trunk.

9. Cisco Unified Communications Manager terminates recording of the customer voice by sending a BYE message to the recorder through a SIP trunk.

10. Party B calls party D (another far-end party = agent in local cluster).

11. Party D answers the call from party B.

12. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager makes a recording call to the built-in bridge (BIB) of the party B IP phone for the agent voice.

13. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B IP phone for the customer voice.

14. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.

15. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the party A (customer) voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.

16. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager makes a recording call to the built-in bridge (BIB) of the party D IP phone for the agent voice.

17. Cisco Unified Communications Manager makes the second recording call to the BIB of the party D IP phone for the customer voice.

18. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the party D (agent) voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.

19. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the party A (customer) voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.

20. Party B completes the transfer.

21. Cisco Unified Communications Manager terminates recording of the party B (agent) voice (the consultation call) by sending a BYE message to the recorder through a SIP trunk.

22. Cisco Unified Communications Manager terminates recording of the party A (customer) voice by sending a BYE message to the recorder through a SIP trunk.

23. Because party D is now connected to a new far-end party, party A, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party D (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party A (customer) voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- When the near-end party B presses **Transfer**, the call is implicitly put on hold, and the recording session with party A terminates.
When party B dials party D and party D answers, a new recording session starts for party D.

When party B completes the transfer, party D and party A get connected and the recorder receives an update with information about the new far-end party A.

Generally, each time an agent puts a recording call on hold, the current recording session terminates. Each time the agent invokes a supplementary service, such as Transfer or hold, the call is implicitly put on hold. Each time the far-end information changes, Cisco Unified Communications Manager sends a SIP UPDATE message to the recorder.

Note the header information of the INVITE messages from step 5, step 14, step 18, and the UPDATE message from step 23. The SIP header enhancement feature adds the information in **bold text** to the message headers.

**Step 5 INVITE Message Header Information**

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1

**Step 14 INVITE Message Header Information**

From:
<sip:2000@ucm1;x-nearend;x-refci=ci3;x-nearenddevice=deviceB;x-farendrefci=ci4;x-farenddevice=deviceD;x-farendaddr=2001>;tag=fromtag2

**Step 18 INVITE Message Header Information**

From:
<sip:2001@ucm1;x-nearend;x-refci=ci4;x-nearenddevice=deviceD;x-farendrefci=ci3;x-farenddevice=deviceB;x-farendaddr=2000>;tag=fromtag2

**Step 23 UPDATE Message Header Information**

From:
<sip:2001@ucm1;x-nearend;x-refci=ci4;x-nearenddevice=deviceD;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag2
Far-End Party Transfers Call to CFNA-Enabled Party

In this use case for automatic call recording, the far-end party blind-transfers the call to a party that has Call Forward No Answer (CFNA) enabled. Figure 34-17 illustrates this use case.

**Figure 34-17  Far-End Party Transfers Call to CFNA-Enabled Party**

In this use case, the following entities participate:

- The customer call originates from DN 1000 device A.
- The agent receives the call at DN 2000 device B.
- The customer blind-transfers the call to DN 1100 device C.
- Device C does not answer but has CFNA enabled to forward to DN 1200 device D.

During an automatic call recording session where the far-end party (customer) on the call transfers the call to another far-end party in the same local cluster but the far-end party has CFNA enabled, so the call forwards to a third far-end party in the local cluster, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B (near-end party = agent in local cluster) answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the agent voice stream to the recorder.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.
7. Party A presses **Transfer**, dials DN 1100 device C, and presses **Transfer** again (performs a blind transfer).
8. Cisco Unified Communications Manager rings DN 1100 on device C, but this DN and device have CFNA configured: ringing times out, and Cisco Unified Communications Manager forwards the call to DN 1200 device D.

9. Far-end party D with DN 1200 on device D answers the call.

10. Because party B is now connected to a new far-end party, party D, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

11. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party D (customer) voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

   Note the following particularities of call processing that apply in this use case:

   • For local-cluster transfers, Cisco Unified Communications Manager updates the recorder only when a new far-end party answers.

   • A SIP UPDATE message that contains updated far-end information gets sent to the recorder when party D answers.

   Note the header information of the INVITE messages from step 5 and step 10. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

   **Step 5 INVITE Message Header Information**
   
   From:
   `<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1`

   **Step 10 UPDATE Message Header Information**
   
   From:
   `<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci5;x-farenddevice=deviceD;x-farendaddr=1200>;tag=fromtag1`
Far-End Party in Local Cluster Creates Conference

In this use case for automatic call recording, the far-end party in a local cluster creates a conference. Figure 34-18 illustrates this use case.

Figure 34-18  Far-End Party in Local Cluster Creates Conference

In this use case, the following entities participate:

- The far-end customer call originates from DN 1000 device A.
- The near-end agent receives the call at DN 2000 device B.
- Party A creates a conference by conferencing in DN 1100 device C.

During an automatic call recording session where the far-end (customer) party in the local cluster creates a conference by bringing an additional far-end party into the call, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B (near-end party = agent in local cluster) answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.

6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party A (customer) voice stream to the recorder.

7. Party A initiates a conference by pressing **Conf**n and dialing DN 1100.

8. Party C DN 1100 device C answers the call.

9. Party A completes the conference by pressing **Conf**n again.

10. Because party B is now connected to a new far-end party, CFB_2, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

    The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

11. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for CFB_2 (conference bridge) through a SIP trunk. The agent IP phone forks the conference voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- After the conference gets established, the far-end party is changed to the conference bridge (CFB).
- Cisco Unified Communications Manager sends a SIP UPDATE message to the recorder.

Note the header information of the INVITE messages from step 5 and step 10. The SIP header enhancement feature adds the information in **bold text** to the INVITE message headers.

**Step 5 INVITE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```

**Step 10 UPDATE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci7;x-farenddevice=CFB_2;x-farendaddr=b001234567;isfocus>;tag=fromtag1
```

The UPDATE message in step 10 includes *isfocus*. This *isfocus* indicates that the near-end party is participating in a conference call. The UPDATE message also includes a b-number as the new far-end address. The b-number specifies the DN of the conference bridge (CFB).
Near-End Party in Local Cluster Creates Conference

In this use case for automatic call recording, the near-end party in a local cluster creates a conference. Figure 34-19 illustrates this use case.

Figure 34-19 Near-End Party in Local Cluster Creates Conference

In this use case, the following entities participate:

- The far-end customer call originates from DN 1000 device A.
- The near-end agent receives the call at DN 2000 device B.
- Party B creates a conference by conferencing in DN 1100 device C.

During an automatic call recording session where the near-end (agent) party in the local cluster creates a conference by bringing an additional far-end party into the call, the following steps take place:

1. Party A (far-end party = customer in local cluster) calls party B (near-end party = agent).
2. Party B (near-end party = agent in local cluster) answers the call.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
5. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.

6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party A (customer) voice stream to the recorder.

7. Party B, the near-end party, initiates a conference by pressing **Conf**. When the near-end party makes a consultation call for a conference participant, the near-end party call automatically gets put on hold.

8. Cisco Unified Communications Manager terminates recording of the party B (agent) voice (the consultation call) by sending a BYE message to the recorder through a SIP trunk.

9. Cisco Unified Communications Manager terminates recording of the party A (customer) voice by sending a BYE message to the recorder through a SIP trunk.

10. Near-end party B dials DN 1100 party C.

11. Party C answers the call.

12. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager makes a recording call to the built-in bridge (BIB) of the party B IP phone for the near-end (agent) voice.

13. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B IP phone for the far-end (customer) voice.

14. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone starts to fork the near-end (agent) voice stream to the recorder.

15. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the far-end (customer) voice through a SIP trunk. The agent IP phone starts to fork the customer voice stream to the recorder.

16. Party B completes the consultation conference by pressing **Conf**. All parties connect to the conference bridge (CFB_2).

17. Because party B is now connected to a new far-end party, CFB_2, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

18. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for CFB_2 (conference bridge) through a SIP trunk. The agent IP phone forks the conference voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Near-end party creates a conference; the first recording session gets torn down
- Connection of the consultation call re-establishes the recording session.
- Far-end party changes to CFB and Cisco Unified Communications Manager sends SIP UPDATE message to the recorder.
Introducing Monitoring and Recording

Note the header information of the INVITE messages from step 5 and step 14, and the UPDATE message from step 17. The SIP header enhancement feature adds the information in bold text to the INVITE and UPDATE message headers.

**Step 5 INVITE Message Header Information**
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1

**Step 14 INVITE Message Header Information**
From:
<sip:2000@ucm1;x-nearend;x-refci=ci3;x-nearenddevice=deviceB;x-farendrefci=ci4;x-farenddevice=deviceC;x-farendaddr=1100>;tag=fromtag1

**Step 17 UPDATE Message Header Information**
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci7;x-farenddevice=CFB_2;x-farendaddr=8001234567;isfocus>;tag=fromtag1

The UPDATE message in step 17 includes isfocus. This isfocus indicates that the near-end party is participating in a conference call. The UPDATE message also includes a b-number as the new far-end address. The b-number specifies the DN of the conference bridge (CFB).

**Far-End Party in Remote Cluster Transfers Call to Another Party in Remote Cluster**

In this use case for automatic call recording, the far-end party in a remote cluster transfers the call to another party in the remote cluster. Figure 34-20 illustrates this use case.
In this use case, the following entities participate:

- The customer call originates from DN 3000 device D in cluster Cisco Unified CM2.
- The agent receives the call at DN 2000 device B in cluster Cisco Unified CM1.
- Agent D transfers the call to DN 3100 device E in cluster Cisco Unified CM2.

During an automatic call recording session where the far-end (agent) party in the remote cluster transfers the call to another party in the remote cluster, the following steps take place:

1. Party D (far-end party = customer in remote cluster) calls party B (near-end party = agent) in local cluster by dialing 82000.
2. The remote cluster (Cisco Unified CM2) sends an INVITE message to the local cluster (Cisco Unified CM1) through a SIP trunk. The message contains information about party D.
3. Party B (near-end party = agent in local cluster) answers the call.
4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.
7. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party D (customer) voice stream to the recorder.
8. Party D in the remote cluster initiates a transfer (presses Transfer) and dials DN 3100 device E, which is also in the remote cluster.
9. Party E answers the call.
10. Party D completes the transfer by pressing Transfer.
11. The remote cluster (Cisco Unified CM2) sends an INVITE message to the local cluster (Cisco Unified CM1) through a SIP trunk. The message contains information about party E.
12. Because party B is now connected to a new far-end party, party E, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

13. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party E (customer) voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Far-end party and transfer-to party are both in the remote (Cisco Unified CM2) cluster. The near-end party sees the far-end party via the SIP trunk that links the two clusters.
- When the transfer-to party answers, the recorder receives an UPDATE message that contains the far-end address.
Note the header information of the INVITE message from step 6 and the UPDATE message from step 12. The SIP header enhancement feature adds the information in **bold text** to the message headers.

**Step 6 INVITE Message Header Information**

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=SIPTrunkTocluster2;x-farendaddr=3000>;tag=fromtag1

**Step 12 UPDATE Message Header Information**

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=SIPTrunkTocluster2;x-farendaddr=3100>;tag=fromtag1

**Far-End Party in Remote Cluster Blind-Transfers Call to Remote-Cluster Party That Has CFNA Configured**

In this use case for automatic call recording, the far-end party in the remote cluster blind-transfers the call to a remote party that does not answer and has Call Forward No Answer (CFNA) configured. **Figure 34-21** illustrates this use case.

**Figure 34-21 Far-End Party in Remote Cluster Blind-Transfers Call to Remote-Cluster Party That Has CFNA Configured**

In this use case, the following entities participate:

- The customer call originates from DN 3000 device D in cluster Cisco Unified CM2.
- The agent receives the call at DN 2000 device B in cluster Cisco Unified CM1.
- Agent D blind-transfers the call to DN 3100 device E in cluster Cisco Unified CM2.
- Agent E does not answer and the call forwards to DN 3200 device F in cluster Cisco Unified CM2.

During an automatic call recording session where the far-end (agent) party in the remote cluster blind-transfers the call to another party in the remote cluster, but the second party does not answer and the call forwards to a third party in the remote cluster, the following steps take place:

1. Party D (far-end party = customer in remote cluster) calls party B (near-end party = agent) in local cluster by dialing 82000.
2. The remote cluster (Cisco Unified CM2) sends an INVITE message to the local cluster (Cisco Unified CM1) through a SIP trunk. The message contains information about party D.

3. Party B (near-end party = agent in local cluster) answers the call.

4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.

5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.

6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.

7. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party D (customer) voice stream to the recorder.

8. Party D in the remote cluster initiates a transfer (presses Transfer) and dials DN 3100 device E, which is also in the remote cluster.

9. Party E does not answer the call: ringing times out, so Cisco Unified Communications Manager sends the call to party F DN 3200 device F.

10. The remote cluster (Cisco Unified CM2) sends an UPDATE message to the local cluster (Cisco Unified CM1) through a SIP trunk. The message contains information about party E.

11. Because party B is now connecting to a new far-end party, party E, local Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

12. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party E (customer) voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

13. Party F answers the forwarded call.

14. The remote cluster (Cisco Unified CM2) sends an UPDATE message to the local cluster (Cisco Unified CM1) through a SIP trunk. The message contains information about party F.

15. Because party B is now connected to a new far-end party, party F, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

16. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party F (customer) voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Far-end part D in remote cluster transfers call to party E in remote cluster; the remote Cisco Unified Communications Manager updates the recorder.

- Party E CFNA timer expires and Cisco Unified Communications Manager redirects call to party F; the remote Cisco Unified Communications Manager again updates the recorder.
The call state of the local Cisco Unified Communications Manager remains call-active, so Cisco Unified Communications Manager updates the recorder for each forwarded remote device.

Note the header information of the INVITE messages from step 6, step 11, and step 15. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

### Step 6 INVITE Message Header Information

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddev
ice=SIPTrunkTocluster2;x-farendaddr=3000>;tag=fromtag1
```

### Step 11 UPDATE Message Header Information

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddev
ice=SIPTrunkTocluster2;x-farendaddr=3100>;tag=fromtag1
```

### Step 15 UPDATE Message Header Information

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddev
ice=SIPTrunkTocluster2;x-farendaddr=3200>;tag=fromtag1
```

## Far-End Party in Remote PBX Transfers Call to Phone in Local Cluster

In this use case for automatic call recording, the far-end party in a remote PBX transfers a call to a phone in the local cluster. **Figure 34-22** illustrates this use case.
In this use case, the following entities participate:

- The customer call originates from DN 3000 device D in PBX1.
- The agent receives the call at DN 2000 device B in cluster Cisco Unified CM1.
- Agent D transfers the call to DN 1000 device A in cluster Cisco Unified CM1.

During an automatic call recording session where the far-end (agent) party in a remote PBX transfers the call to another party in the local cluster, the following steps take place:

1. Party D (far-end party = customer in remote PBX) calls party B (near-end party = agent) in local cluster by dialing 82000.
2. The remote PBX sends an setup message to the local cluster (Cisco Unified CM1) through a PRI QSIG gateway. The message contains information about party D.
3. Party B (near-end party = agent in local cluster) answers the call.
4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.
7. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the particle D (customer) voice stream to the recorder.
8. Party D in the remote PBX initiates a consultation transfer (presses Transfer) and dials DN 81000 device A, which is in the local cluster.
9. The remote PBX sends an setup message to the local cluster (Cisco Unified CM1) through a PRI QSIG gateway. The message contains information about party D.
10. Party A answers the call from party D.
11. Party D presses Transfer to complete the transfer.
12. Remote PBX sends UPDATE.
13. Remote PBX sends UPDATE.
14. Because party B is now connecting to a new far-end party, party A, local Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.
15. The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party A (customer) voice. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- When the far-end party in a remote cluster transfers the call to a party in the local cluster, Cisco Unified Communications Manager sends a SIP UPDATE message with farendaddr for the transferred-to local-cluster party.
• This transfer specifies a hairpin transfer: the far-end address changed to the local DN 1000 in the UPDATE message.

Note the header information of the INVITE messages from step 6 and step 14. The SIP header enhancement feature adds the information in bold text to the INVITE and UPDATE message headers.

Step 6 INVITE Message Header Information

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddev
ice=PriQSIGGW;x-farendaddr=3000>;tag=fromtag1

Step 14 UPDATE Message Header Information

From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddev
ice=PriQSIGGW;x-farendaddr=1000>;tag=fromtag1

Remote PBX Far-End Party Transfers Call to Local Phone With Path Replacement

In this use case for automatic call recording, a remote PBX far-end party transfers the call to a local phone by using path replacement. Figure 34-23 illustrates this use case.

Figure 34-23 Remote PBX Far-End Party Transfers Call to Local Phone With Path Replacement

In this use case, the following entities participate:
• The customer call originates from DN 3000 device D in PBX1.
• The agent receives the call at DN 2000 device B in cluster Cisco Unified CM1.
• Agent D transfers the call to DN 1000 device A in cluster Cisco Unified CM1.

During an automatic call recording session where the far-end (agent) party in a remote PBX transfers the call to a phone in the local cluster by using path replacement, the following steps take place:
1. Party D (far-end party = customer in remote PBX) calls party B (near-end party = agent) in local cluster by dialing 82000.
2. The remote PBX sends an setup message to the local cluster (Cisco Unified CM1) through a PRI QSIG gateway. The message contains information about party D.
3. Party B (near-end party = agent in local cluster) answers the call.

4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.

5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.

6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.

7. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party D (customer) voice stream to the recorder.

8. Party D in the remote PBX initiates a consultation transfer (presses Transfer) and dials DN 81000 device A, which is in the local cluster.

9. The remote PBX sends an setup message to the local cluster (Cisco Unified CM1) through a PRI QSIG gateway. The message contains information about party D.

10. Local party A answers the call from party D.

11. Remote party D presses Transfer to complete the transfer.

12. Remote PBX sends UPDATE.

13. Remote PBX sends UPDATE.

14. Because party B is now connecting to a new far-end party, party A, local Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

15. The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party A (customer) voice. The agent IP phone forks the customer voice stream to the recorder.

16. Local Cisco Unified Communications Manager initiates path replacement process directly connects device A with device B and eliminates routing through the remote PBX.

17. Because party B is now connecting to a new far-end party, party A, local Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

18. The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party A (customer) voice. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Path replacement replaces a hairpin call to remote PBX so that party A and party B are directly connected without routing through the remote PBX.
- The far-end call information gets updated when transfer completes.
- When path replacement completes, the far-end device also gets updated.
Note the header information of the INVITE messages from step 6, step 14, and step 17. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

**Step 6 INVITE Message Header Information**
```
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=PriQSIGGW;x-farendaddr=3000>;tag=fromtag1
```

**Step 14 UPDATE Message Header Information**
```
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=PriQSIGGW;x-farendaddr=1000>;tag=fromtag1
```

**Step 17 UPDATE Message Header Information**
```
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci4;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```

**Far-End Party Transfers Call Across DMS Gateway**

In this use case for automatic call recording, the far-end party transfers a call across a DMS gateway. *Figure 34-24* illustrates this use case.

**Figure 34-24  Far-End Party Transfers Call Across DMS Gateway**
Introducing Monitoring and Recording

In this use case, the following entities participate:

- The customer call originates from DN 9725550001 device D that connects to a DMS switch.
- The agent receives the call at DN 2000 device B in cluster Cisco Unified CM1.
- Agent D transfers the call to DN 9725550002 device E that connects to a DMS switch.

During an automatic call recording session where the far-end (agent) party that connects through a DMS switch transfers the call to a phone that also connects through a DMS switch, the following steps take place:

1. Party D (far-end party = customer across DMS switch) calls party B (near-end party = agent) in local cluster by dialing 82000.
2. The DMS switch sends a PriSetup message to the local cluster (Cisco Unified CM1) through a PRI DMS gateway. The message contains information about party D.
3. Party B (near-end party = agent in local cluster) answers the call.
4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
6. The recorder receives and answers the recording call setup messages that are sent from local Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.
7. The recorder receives and answers the recording call setup messages that are sent from local Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party D (customer) voice stream to the recorder.
8. Party D across the DMS gateway initiates a consultation transfer (presses Transfer) and dials DN 9725550002 device E, which is also across the DMS gateway.
9. Party E answers the call from party D.
10. The DMS switch sends a PriNotify message to the local cluster (Cisco Unified CM1) through a PRI DMS gateway. The message contains information about party E.
11. Because party B is now connecting to a new far-end party, party E, local Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

12. The recorder receives and answers the recording call UPDATE message that is sent from local Cisco Unified Communications Manager for the party E (customer) voice. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- In general, when a far-end party on the PSTN side transfers a call, Cisco Unified Communications Manager does not know about the transferring nor transferred-to parties. If the DMS switch or PBX supports PriNotify, however, Cisco Unified Communications Manager receives the PriNotify message when the far-end party changes and can update the far-end information to the recorder.
Note the header information of the INVITE messages from step 6 and step 11. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

**Step 6 INVITE Message Header Information**
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=PriDMSGW;x-farendaddr=9725550001>;tag=fromtag1

**Step 11 UPDATE Message Header Information**
From:
<sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=PriDMSGW;x-farendaddr=9725550002>;tag=fromtag1

**Desktop Pickup of Mobile Phone Call**

In this use case for automatic call recording, mobile phone user sends call to desk phone for pickup. **Figure 34-25** illustrates this use case.

**Figure 34-25  Desktop Pickup of Mobile Phone Call**

In this use case, the following entities participate:

- The customer call originates from mobile device UserACell, enterprise extension 1000 and mobile number 9725551000.
- The agent receives the call at DN 2000 device B.
- The customer resumes the call from the customer enterprise phone DN 1000 device A.

During an automatic call recording session where desktop pickup of a mobile phone call occurs, the following steps take place:

1. UserACell calls party B DN 2000 device B.
2. Cisco Unified Mobile Communicator client sends SETUP message
3. SETUP message travels through H.323 gateway to local Cisco Unified CM1 cluster.
4. Party B answers the incoming call from UserACell.
5. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.

6. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.

7. The recorder receives and answers the recording INVITE messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.

8. The recorder receives and answers the recording INVITE messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party UserACell (customer) voice stream to the recorder.

9. UserACell presses **Enterprise Hold** on the user A mobile phone.

10. User A presses **Resume** on the user A desk phone.

11. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

12. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- Mobile phone uses the shared-line concept. When the mobile phone call gets put on hold and the desktop phone resumes the call, the far-end party changes. Cisco Unified Communications Manager sends an update to the recorder.

- The user picks up the call from the user desk phone to continue the conversation that started on the user mobile phone. To do so, use Cisco Unified Communications Manager to place the call on hold (enterprise hold) through the mobile phone data channel; then, resume the call from the desk phone.

Note the header information of the INVITE messages from step 7 and step 11. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

**Step 7 INVITE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=UserACell;x-farendaddr=1000>;tag=fromtag1
```

**Step 11 UPDATE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```
Far-End Party Sends Call to Mobile Phone for Mobile Phone Pickup

In this use case for automatic call recording, the far-end party sends a call to the user mobile phone for mobile phone pickup. (This scenario specifies the opposite of the scenario that the “Desktop Pickup of Mobile Phone Call” section on page 34-44 specifies.) Figure 34-26 illustrates this use case.

In this use case, the following entities participate:

- The customer call originates from DN 1000 device A.
- The agent receives the call at DN 2000 device B.
- The customer resumes the call from the customer mobile phone device UserACell enterprise extension 1000 mobile number 9725551000.

During an automatic call recording session where an enterprise user sends a call to the user mobile phone, the following steps take place:

1. Enterprise user far-end party A calls party B DN 2000 device B from DN 1000 device A.
2. Party B DN 2000 answers the incoming call from far-end party A.
3. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
4. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
5. The recorder receives and answers the recording INVITE messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.
6. The recorder receives and answers the recording INVITE messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party A (customer) voice stream to the recorder.
7. Party A presses Send to Mobile on the user A desk phone.
8. Cisco Unified Communications Manager sends a Setup message to the User A mobile phone.
9. User A presses answers the ringing call on device UserACell.

10. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.

11. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone forks the customer voice stream to the recorder.

Note the following particularities of call processing that apply in this use case:

- When party UserACell answers the call, the party UserACell information is sent in a SIP UPDATE message to the recorder.

Note the header information of the INVITE messages from step 5 and step 10. The SIP header enhancement feature adds the information in **bold text** to the INVITE and UPDATE message headers.

**Step 5 INVITE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=deviceA;x-farendaddr=1000>;tag=fromtag1
```

**Step 10 UPDATE Message Header Information**

```
From: <sip:2000@ucm1;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci3;x-farenddevice=UserACell;x-farendaddr=1000>;tag=fromtag1
```

**Far-End Party in Remote Cluster Creates Conference**

In this use case for automatic call recording, the far-end party in a remote cluster creates a conference. **Figure 34-27** illustrates this use case.
In this use case, the following entities participate:

- The far-end customer call originates from DN 3000 device D.
- The near-end agent receives the call at DN 2000 device B.
- Party D creates a conference by conferencing in DN 3100 device E.

During an automatic call recording session where the far-end party in a remote cluster creates a conference, the following steps take place:

1. Party D (far-end party = customer in remote cluster) calls party B (near-end party = agent) by dialing 82000.
2. The INVITE message passes over the SIPTrunkToCluster2 SIP trunk.
3. Party B (near-end party = agent in local cluster) answers the call.
4. Because the agent line appearance is configured for automatic recording, the recording session for the media streams automatically gets triggered. Cisco Unified Communications Manager first makes a recording call to the built-in bridge (BIB) of the party B (agent) IP phone for the agent voice.
5. Cisco Unified Communications Manager makes the second recording call to the BIB of the party B (agent) IP phone for the customer voice.
6. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the agent voice through a SIP trunk. The agent IP phone starts to fork the party B (agent) voice stream to the recorder.
7. The recorder receives and answers the recording call setup messages that are sent from Cisco Unified Communications Manager for the customer voice through a SIP trunk. The agent IP phone starts to fork the party D (customer) voice stream to the recorder.
8. Party D initiates a conference by pressing Confn and dialing DN 3100.
9. Party E DN 3100 device E answers the call.
10. Party D completes the conference by pressing Confn again.
11. The UPDATE message passes over the SIPTrunkToCluster2 SIP trunk.
12. Because party B is now connected to a new far-end party, CFB_2, Cisco Unified Communications Manager sends two UPDATE messages to the recorder.

   The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for the party B (agent) voice through a SIP trunk. The agent IP phone forks the agent voice stream to the recorder.
13. The recorder receives and answers the recording call UPDATE message that is sent from Cisco Unified Communications Manager for CFB_2 (conference bridge) through a SIP trunk. The agent IP phone forks the conference voice stream to the recorder.

Note the following particularities of call processing and configuration that apply in this use case:

- Cisco Unified Communications Manager has very limited view if a far-end party creates a conference in a remote cluster. The far-end party device is always the trunk that links the two clusters.
- After the remote conference gets established, the remote Cisco Unified CM2 cluster delivers the b-number (conference bridge identifier) in the SIP UPDATE to the local cluster, Cisco Unified CM1. The Cisco Unified CM1 cluster sends the update to the recorder with the b-number and isfocus indicator.
In the figure, the Cisco Unified CM1 cluster gets configured with a SIP trunk, SIPTrunkToCluster2, that links the Cisco Unified CM1 cluster to the Cisco Unified CM2 cluster. The corresponding SIP trunk that is configured in the Cisco Unified CM2 cluster specifies SIPTrunkToCluster1.

When the conference gets created by the far-end party with DN 3000, the conference bridge identifier, b001234567, does not get passed to cluster Cisco Unified CM1 by default. If the identifier is not passed, the Cisco Unified CM1 cluster can still include the isfocus flag for the far-end party in the From header to the recorder, but the far-end party address will be empty.

To allow the conference bridge identifier (the b-number of the conference bridge) to pass from cluster Cisco Unified CM2 to cluster Cisco Unified CM1, the administrator creates a SIP profile in cluster Cisco Unified CM2, checks the Deliver Conference Bridge Identifier check box, and assigns the SIP profile to SIPTrunkToCluster1 in cluster Cisco Unified CM2. The administrator also creates a SIP profile in cluster Cisco Unified CM1 and assigns this SIP profile to the SIPTrunkToCluster2 in cluster Cisco Unified CM1.

For more details about configuring SIP profiles, see the “SIP Profile Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

Note the header information of the INVITE messages from step 6 and step 12. The SIP header enhancement feature adds the information in bold text to the INVITE and UPDATE message headers.

**Step 6 INVITE Message Header Information**

```
From: <sip:2000@ucml;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=SIPTrunkToCluster2;x-farendaddr=3000>;tag=fromtag1
```

**Step 12 UPDATE Message Header Information**

```
From: <sip:2000@ucml;x-nearend;x-refci=ci2;x-nearenddevice=deviceB;x-farendrefci=ci1;x-farenddevice=SIPTrunkToCluster2;x-farendaddr=b001234567;isfocus>;tag=fromtag1
```

The UPDATE message in step 12 includes isfocus. This isfocus indicates that the near-end party is participating in a conference call. The UPDATE message also includes a b-number as the new far-end address. The b-number specifies the DN of the conference bridge (CFB).

**Application-Invoked Recording**

In application-invoked recording, when an agent call becomes active, the application can send a Start Recording command for the call. Be aware that recording calls setup is identical to the setup for automatic recording.
Introducing Monitoring and Recording

Figure 34-28 illustrates application-invoked recording.

**Figure 34-28  Application-Invoked Recording**

A supervisor or an authorized person can start a call recording session for an active call after the call becomes active. Figure 34-28 shows such an example. In this case, the supervisor detected the agent is on an active call, and the supervisor clicks the record button on the recording application for the call. The application sends a Start Recording command to Cisco Unified Communications Manager with the call information. Cisco Unified Communications Manager then establishes two recording calls from the agent IP phone to the recorder for the two voice streams of the call.

**Recording Calls Do Not Survive Agent Hold**

Recording calls get torn down when the agent puts the call on hold, and they get reestablished when the agent resumes the call.

The Start Recording Request from an application persists throughout the call.
Figure 34-29 illustrates the scenario in which recording calls do not survive agent hold.

Figure 34-29  Recording Calls Do Not Survive Agent Hold

- Customer voice
- Agent voice

1. Customer voice
2. (disconnect)
3. (disconnect)

1. Resume
2. (setup)
3. (setup)
Recording a Barged Call

When recording a barged call, the following recording streams apply: the customer voice alone and the mixed voices of agent 1 and agent 2.

Figure 34-30 illustrates the scenario when a barged call is recorded.

Recording an Agent Conference

When a conference is recorded, the following recording streams apply: agent voice alone and the mixed voices from the rest of the conference participants.

An agent may create a conference while being recorded. During the conference setup process, recording calls get torn down and then reestablished.
Figure 34-31 illustrates the scenario in which an agent conference gets recorded.

**Figure 34-31   Agent’s Conference Gets Recorded**

- mix of agent 2 voice and customer voice
- agent 1 voice
Simultaneous Monitoring and Recording

Recording can take place when the agent call is being monitored. Recording and monitoring get set up independently from each other. Figure 34-32 illustrates simultaneous monitoring and recording.

In the case of simultaneous monitoring and recording, the following steps take place:

1. A customer calls into the call center.
2. The call routes to agent. Agent answers the call. A two-way media streaming gets set up between agent IP phone and the customer.
3. The recording call for the agent voice gets set up between agent phone and the recorder.
4. The recording call for the customer voice gets set up between agent phone and the recorder.
5. The supervisor desktop application shows that agent has an active call. On his desktop application, the supervisor clicks the monitor button for current active call of agent.
6. The supervisor IP phone gets triggered to go off hook and make a monitoring call toward agent.
7. Agent phone accepts the monitoring call. Agent phone starts to send a stream of mixed voices of the customer and the agent to the supervisor IP phone. Neither the agent nor the customer can hear the supervisor.
Call Characteristics of Monitoring and Recording Calls

The topics in this section describe various characteristics of monitoring and recording calls. This section covers the following topics:

- Monitoring and Recording Notification Tones, page 34-55
- Play Tone Behavior, page 34-55
- Codec for Monitoring and Recording Calls, page 34-56
- Limit Codec Usage for Recording Calls, page 34-56
- Monitoring and Recording Are One-Way Media, page 34-57
- One-Way Media and Firewalls, page 34-57
- Call Preservation in Monitoring and Recording, page 34-58

Monitoring and Recording Notification Tones

In certain jurisdictions, a requirement exists to inform the agent or the customer that their call is being monitored or reordered in the form of tones.

Use the following service parameters to set the default play tone options:

- Play Recording Notification Tone To Observed Target
- Play Recording Notification Tone To Observed Connected Parties
- Play Monitoring Notification Tone To Observed Target
- Play Monitoring Notification Tone To Observed Connected Parties

The application also provides the tone option in the monitoring or recording request. The tone plays when either the server parameter or application enables tones.

Figure 34-33 illustrates the observed connected party and the observed target.

Play Tone Behavior

Monitoring tone and recording tone represent two different tones; they can be enabled or disabled separately.

By default, the supervisor does not hear monitoring or recording tones. Playing to the supervisor can be enabled optionally through the device recording tone setting.
Table 34-2 specifies the behavior of tones in monitoring and recording scenarios.

<table>
<thead>
<tr>
<th>Play To</th>
<th>Agent Hears</th>
<th>Customer Hears</th>
<th>Supervisor Monitoring Stream</th>
<th>Agent Recording Stream</th>
<th>Customer Recording Stream</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Agent</td>
<td>Tone</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Customer</td>
<td>None</td>
<td>Tone</td>
<td>None</td>
<td>Tone</td>
<td>None</td>
</tr>
<tr>
<td>Both</td>
<td>Tone</td>
<td>Tone</td>
<td>None</td>
<td>Tone</td>
<td>None</td>
</tr>
</tbody>
</table>

**Codec for Monitoring and Recording Calls**

The agent device and the supervisor device negotiate the codec for a monitoring call, subject to Cisco Unified Communications Manager region settings.

The codecs for recording calls match the codec of the customer-agent call. Figure 34-34 illustrates the codecs for monitoring and recording calls.

**Limit Codec Usage for Recording Calls**

Because the codecs for recording calls match the codecs for agent-customer calls, you may need to insert transcoders if the recorder does not support the matching codecs.

Cisco Unified IP Phones adds new codecs that Cisco transcoders do not support.
Use the following service parameters to enable or disable usage of the G722 and iLBC codecs:

- G722 Codec Enabled
- iLBC Codec Enabled

Find these service parameters in the Clusterwide Parameters (System - Location and Region) section of the Service Parameter Configuration window.

You can set these service parameters with the following values:

- Enabled for All Devices
- Enabled for All Devices Except Recording-Enabled Devices
- Disabled

**Monitoring and Recording Are One-Way Media**

A monitoring call comprises one-way media from an agent phone to a supervisor phone.

Recording calls comprise one-way media from an agent phone to the recorder.

Monitoring calls and recording calls go through normal call admission control; however, each of the streams leaving the BIB destined for the recorder use the same calculations as the two-way media.

NAT separating agent and supervisor or agent and recorder remain transparent to the monitoring or recording calls (within the limitations of Cisco Unified Communications Manager).

**One-Way Media and Firewalls**

Firewall software needs to know the destination IP address and destination port as well as the source IP address to open the pinhole for an RTP stream.

Be aware that SCCP messages for media are not symmetric, SIP is OK.

The SCCP ver 12 enhancement for one-way media provides the following additions:

- New StartMediaTransmissionAck (SMTACK) message with transmission IP and port
- OpenReceiveChannel (ORC) with additional transmission IP and port

Figure 34-35 illustrates the issue with one-way media and a firewall.
Call Preservation in Monitoring and Recording

If the agent call that is being monitored or recorded goes to call preservation, Cisco Unified Communications Manager puts the monitoring call or recording calls into call preservation mode.

The agent call does not get affected if the monitoring call or recording call go to call preservation mode.

Call Information and Call Display

Built-in Bridge (BIB) specifies a component in the device layer. BIB provides the logical representation of the DSP resource in the Cisco Unified IP Phone. Calls that are made to the BIB of the phone device layer remain hidden to the user.

Monitoring and recording calls (the server calls) to the agent get made to the BIB of the agent.

For a monitoring call, the supervisor phone displays “From Monitoring [agent user name/DN].”

For a recording call to the recorder, the special tag in the “from header” of the SIP INVITE message indicates the source of the voice stream.

For Agent Voice

From “AgentUserName” <sip:agentDN@ccm;x-nearend;x-refCI=12345;x-nearenddevice=[agent_devicename]”

For Customer Voice

From “AgentUserName” <sip:agentDN@ccm;x-farend;x-refCI=12345;x-farenddevice=[farend_devicename]”
CTI Event Delivery to Application

CTI Events get delivered to the agent on the primary call leg (or reference call leg), as shown in Figure 34-36.

System Requirements for Monitoring and Recording

The following sections provide the system requirements for monitoring and recording.

CTI Requirements

Computer Telephony Integration (CTI) provides the ability for applications to monitor calls on a per-call basis. Cisco defines the monitor target as the party that is monitored and the monitor initiator as the monitoring party.

If a single application observes both the monitor target and the monitor initiator, call events that get reported to the application help the application identify calls on the monitor target and provide the ability to monitor the calls. If different applications observe the monitor target and the monitor initiator, the application that observes the monitor target must provide the call information to the application that observes the monitor initiator. Based on the call information that is available to the application that observes the monitor initiator, a monitoring request can get initiated. Termination of the call at the monitor initiator or monitor target stops the monitoring session.
For recording, Cisco Unified Communications Manager provides the ability to record all calls automatically. The SIP or SCCP station initiates this automatic recording and is based on configuration of Cisco Unified Communications Manager Administration. Administrators can configure no recording, can configure automatic recording of all calls, or can configure per-call recording through application control for a line appearance. CTI does not provide the ability to override the administrator configuration in the database.

When the recording type is set to the application-controlled call-based recording, applications can initiate recording on a per-call basis.

When invoking recording and monitoring or any other CTI features, delays and unexpected behavior can result if UDP transport is used for phones that are running SIP.

Applications that intend to monitor or record calls should have the corresponding monitoring and recording privileges enabled for the application user or end user that the application uses.

For convenience the MonitoringPartyInfo, MonitoredPartyInfo, and RecordPartyInfo all get combined and reported as CallAttributeInfo from CTI to applications.

**Hardware Requirements**

The monitoring and recording features support a limited set of phones and related devices. See the “Devices That Support Call Monitoring and Call Recording” section on page 34-6 for details.

**Interactions and Limitations**

This section provides the interactions and limitations for the monitoring and recording feature. See the following topics:

- Interactions, page 34-60
- Limitations, page 34-61

**Interactions**

Monitoring and recording interact with the following applications and features:

- CTI and JTAPI/TSP Applications, page 34-60
- Other Cisco Unified Communications Manager Features, page 34-61

**CTI and JTAPI/TSP Applications**

Computer Telephony Integration (CTI), Java Telephony API (JTAPI), and TSP support monitoring and recording of calls. Applications can use these interfaces to monitor or record calls in a Cisco Unified Communications Manager system.

The initial implementation of this feature presents some limitations. For monitoring, applications must open the line that is to be monitored and the party that will monitor. This requirement exists because the call ID of the call to be monitored should get provided when the monitoring party initiates a request to monitor that call. One way to circumvent this limitation involves using two coordinating applications,
one application to open the line for the monitored party and another application to open the line of the monitoring party, and provide the call ID of the party to be monitored through an out-of-band mechanism. Applications such as IPCC Enterprise use the latter approach.

No backward compatibility implications exist because monitoring and recording as new features do not affect any of the existing features.

**Other Cisco Unified Communications Manager Features**

The following features work transparently with monitoring and recording:
- Forced Authorization Codes (FAC) and Client Matter Codes (CMC)
- QSIG
- Multilevel Precedence and Preemption (MLPP)
- External Call Control

The following features and other Cisco Unified Communications Manager components interact with monitoring and recording:
- Call Transfer
- Immediate Divert (i-Divert)
- Call Park
- Barge
- Music On Hold (MOH)
- Conferencing
- Bulk Administration Tool (BAT)

**Limitations**

The following restrictions and limitations exist for monitoring and recording:
- Codec Consideration During Monitoring or Recording, page 34-61
- Security Handling in Monitoring and Recording, page 34-62
- Intercom, page 34-62
- Recording and Call Hold and Resume, page 34-62
- Recording and Call Park and Retrieve, page 34-62
- Recording and Call Forward No Answer (CFNA), page 34-62
- Recording and Conference Chaining, page 34-63
- Using Route List and/or Multiple Destination Addresses on a SIP Trunk for Multiple Recorders, page 34-63

**Codec Consideration During Monitoring or Recording**

The codec of the call leg that originates from the IP phone that is being monitored or recorded must remain the same throughout the call.
Security Handling in Monitoring and Recording
Cisco Unified Communications Manager allows a supervisor or administrator to monitor a conversation between an agent and a customer without either party knowing that they are being monitored. For information about using and configuring secure call monitoring and recording, see the “Secure Call Monitoring and Recording” chapter in the *Cisco Unified Communications Manager Security Guide*.

Intercom
The system does not allow monitoring nor recording of whisper intercom and talkback intercom calls. Configuration of the intercom calling search space (CSS) specifies this limitation.

Recording and Call Hold and Resume
Cisco Unified Communications Manager does not update the recorder when the far-end party puts the call on hold. The recorder will be updated only when a different far-end party resumes the call.
Cisco Unified Communications Manager updates a recorder when the far-end call information changes. The far-end call information contains a call ID, directory number, and device name. If one of these parameters changes, the far-end call information changes.
If a far-end party holds and resumes a call from the same device, Cisco Unified Communications Manager does not update a recorder.

Recording and Call Park and Retrieve
If the far-end party in a remote cluster parks the call, Cisco Unified Communications Manager updates the recorder with an empty far-end party address, provided the remote cluster connects to the local cluster via a SIP trunk or an H323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the far-end party retrieves the call either from the same or a different device. Cisco Unified Communications Manager does not update the recorder if the far-end party that parks the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the call gets retrieved from a different device.
For remote Call Park and Retrieve, the remote Cisco Unified Communications Manager sends the display name Call Park update. This update contains an empty directory number/address; therefore, the far-end address changes to empty. Due to the far-end address change, the local Cisco Unified Communications Manager sends the update with the empty far-end address to the recorder.

Recording and Call Forward No Answer (CFNA)
If the far-end party in a remote cluster blind-transfers the call to a party that has CFNA enabled, Cisco Unified Communications Manager updates the recorder with the ringing party as the far-end party address, provided the remote cluster connects to the local cluster with a SIP trunk or an H.323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the call gets forwarded to the CFNA target. Cisco Unified Communications Manager does not update the recorder if the far-end party that blind-transfers the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the CFNA target answers the call.
When a remote call becomes active, the call state stays active in a local cluster. When a remote far-end party performs a blind call transfer to a new remote far-end party and the party rings, the local Cisco Unified Communications Manager still sees the call state as active. Thus, for remote Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder for a new party because the call state is active.
When a local call becomes active, the call state can change from active to ringing state. The local Cisco Unified Communications Manager can find out a current call state. Thus, for local Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder after a new far-end party answers a call.
Recording and Conference Chaining

If two or more near-end parties are in two or more conferences that are chained together, Cisco Unified Communications Manager can only update the recorder that they are using; separate conferences are identified by the different conference identifiers (b-number). The conference chaining information can be obtained via Call Detailed Records (CDRs).

Cisco Unified Communications Manager sends UPDATE messages to a recorder if the far-end call information changes. For a conference case, the far-end party address specifies the b-number. If the far-end b-number remains unchanged, Cisco Unified Communications Manager does not send the UPDATE messages to the recorder.

Using Route List and/or Multiple Destination Addresses on a SIP Trunk for Multiple Recorders

When using a route list and/or multiple destination addresses on a SIP trunk for multiple recorders, the near-end and far-end recording calls of the same recording session can go to different recorders.

If a Cisco Unified Communications Manager administrator configures a route list with multiple SIP trunks such that each SIP trunk points to a different recorder, Cisco Unified Communications Manager may not send the two recording calls of a recording session to the same SIP trunk, or to the same recorder. Depending on the selection algorithm that is provisioned in the route group, the likelihood of the two recording calls being sent to the same recorder may vary considerably. Similarly, Cisco Unified Communications Manager may not send the two recording calls to the same recorder if the administrator provisioned multiple IP addresses on a SIP trunk such that each IP address points to a different recorder. In this case, the calls get sent to the recorder that is randomly selected from the provisioned IP addresses.

To configure Cisco Unified Communications Manager to support a recorder cluster configuration where a recording session may be redirected to another of the recorders in the cluster, configure a route list or provision multiple destinations on the recording SIP trunk.

Configuring Monitoring and Recording

The following subsections provide detailed examples of the steps that are necessary to configure monitoring and recording. The configuration checklist in Table 34-1 summarizes the steps in a single table and points to additional Cisco Unified Communications Manager documentation that discusses each menu option in detail.

Use the following topics to configure call monitoring and call recording:

- Turn on IP Phone BIB to Allow Monitoring or Recording, page 34-64
- Add User for Monitoring or Recording Application, page 34-64
- Add User to Groups That Allow Monitoring and Recording, page 34-65
- Configure Tones for Monitoring or Recording (Optional), page 34-66
- Configure Monitoring Calling Search Space, page 34-67
- Enable Recording for a Line Appearance, page 34-68
- Create Recording Profile, page 34-69
- Create SIP Profile for Recording (Optional), page 34-70
- Create a SIP Trunk That Points to the Recorder, page 34-71
- Create a Route Pattern for the Recorder, page 34-72
- Create Recorder Redundancy, page 34-73
Tip

Before you configure monitoring and recording, review the “Configuration Checklist for Monitoring and Recording” section on page 34-1.

Turn on IP Phone BIB to Allow Monitoring or Recording

The built-in bridge of the agent phone must be set to *On* to allow its calls to be monitored or recorded. You can also set the Built-in Bridge Enable service parameter to *On* and leave the Built-in Bridge in the Phone Configuration window set to *Default*.

Use the **Device > Phone** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 34-37 illustrates turning on the IP phone BIB to allow monitoring or recording.

Add User for Monitoring or Recording Application

You must first create the application user who is capable of invoking monitoring or recording, and the application user must belong to a group with monitoring and recording privileges.

Add an application or end user from Application User Configuration window or the End User Configuration window.

Use the **User Management > Application User** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Figure 34-38 illustrates adding a user for the monitoring or recording application.

**Add User to Groups That Allow Monitoring and Recording**

Add the user to the user groups: Standard CTI Allow Call Monitoring user group and the Standard CTI Allow Call Recording user group.

Also add the user to Standard CTI Enabled user group.

Use the **User Management > Application User** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Figure 34-39 illustrates adding the user to these user groups.

Figure 34-39 Adding User to the Appropriate User Groups

Configure Tones for Monitoring or Recording (Optional)

Set the service parameters for playing tone to True to allow tone to be played either to agent only, to customer only, or to both.

Applications that invoke monitoring or recording can also pass the play tone option to Cisco Unified Communications Manager. The monitoring tone or recording tone plays when either the service parameter or the application specifies the play tone option.

Use the System > Service Parameters menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Figure 34-40 illustrates using service parameters to configure tones.

Figure 34-40 Using Service Parameters to Configure Tones

Configure Monitoring Calling Search Space

The monitoring calling search space of the supervisor line appearance must include the agent line or device partition to allow monitoring the agent.

Set the monitoring calling search space on the supervisor line appearance window.

Use the Device > Phone menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration. When you display the Phone Configuration window for a phone, click on a line, such as Line [1], in the Association Information pane. (You can choose either a DN that has already been associated with this phone or you can add a new DN to associate with this phone.) In the Directory Number Configuration window that displays, configure the Monitoring Calling Search Space field for the chosen line on this phone.
Enable Recording for a Line Appearance

To enable recording of an agent, set the Recording Option in the line appearance of the agent to one of the options:

- Automatic Call Recording Enabled
- Application Invoked Call Recording Enabled
- Device Invoked Call Recording Enabled

Select a pre-created recording profile from the drop-down list box. (Use Device > Device Settings > Recording Profile to configure a recording profile.)

Use the Call Routing > Directory Number menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Figure 34-41 illustrates configuring the monitoring calling search space.
Create Recording Profile

Create a recording profile from the Device Setting pull-down menu. Enter the recording profile name, recording calling search space, and recording destination address. Use the Device > Device Settings > Recording Profile menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Create SIP Profile for Recording (Optional)

Create a SIP profile for recording. Use the Device > Device Settings > SIP Profile menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

If you do not create a new SIP profile for recording, you can use the Standard SIP Profile.

You can check the Deliver Conference Bridge Identifier check box, which delivers additional information (specifically, the b-number that identifies a conference bridge) to the recorder across the SIP trunk. If the check box is left unchecked, the far-end information for the remote conference remains empty.

Check the Deliver Conference Bridge Identifier check box on the remote cluster SIP profile as well.

**Note**

Checking this check box is not required for recording, but the conference bridge identifier helps to update the recorder when recording calls that involve a conference bridge.

See the “SIP Profile Configuration” chapter in the Cisco Unified Communications Manager Administration Guide for details of configuring SIP profiles.
Figure 34-44 illustrates creating a SIP profile for recording.

Figure 34-44 Creating a SIP Profile for Recording

Create a SIP Trunk That Points to the Recorder

Create a SIP trunk that points to the recorder.

Enter the recorder DN, which must match a route pattern for the SIP trunk or a route list that includes the recorder.

Choose the appropriate SIP profile that you configured for recording.

Use the Device > Trunk menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Figure 34-45 illustrates creating a SIP trunk that points to the recorder.

**Create a Route Pattern for the Recorder**

Create a route pattern for the recorder SIP trunk. The Recording Destination Address in the recording profile must match this pattern.

Select the SIP trunk that points to the recorder, or select a route list of which the recorder is a member. Use the **Call Routing > Route/Hunt > Route Pattern** menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Create Recorder Redundancy

Many recorders have built-in proxy and redundancy functionalities, for example, Nice/Witness recorders.

You can also use the following mechanism to achieve recorder redundancy:

- Use the SRV record for the recorder destination address in SIP trunk configuration.
- Use multiple recorders for redundancy and load balance. Create a SIP trunk for each recorder; create a route list to include the route groups that have individual SIP trunks as a member.

Use the Device > Trunk menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.
Figure 34-47 illustrates enabling SRV for a SIP trunk.

**Figure 34-47   Enabling SRV for a SIP Trunk**

Setting the Monitoring and Recording Service Parameters

The following service parameters affect the call monitoring and call recording features. These service parameters are classified as the following types:

- Notification, page 34-74
- Codec Usage, page 34-75
- Built-In Bridge, page 34-75

**Notification**

The following service parameters affect the playing of notification tones to the parties that are monitored or recorded by the call monitoring and call recording features:

**Clusterwide Parameters (Feature - Call Recording)**

- Play Recording Notification Tone To Observed Target
- Play Recording Notification Tone To Observed Connected Parties

**Clusterwide Parameters (Feature - Monitoring)**

- Play Monitoring Notification Tone To Observed Target
- Play Monitoring Notification Tone To Observed Connected Parties

The default value for these service parameters specifies `False`. You must change the value of each parameter to `True` to enable the particular notification tone to play.

See the “Monitoring and Recording Notification Tones” section on page 34-55 for more information about these service parameters.
Codec Usage

Use the following service parameters to enable or disable usage of the G722 and iLBC codecs:

Clusterwide Parameters (System - Location and Region)
- G722 Codec Enabled
- iLBC Codec Enabled

See the “Limit Codec Usage for Recording Calls” section on page 34-56 for more information about these service parameters.

Built-In Bridge

The following service parameter enables or disables the built-in bridge on phones:

Clusterwide Parameters (Device - Phone)
- Built-in Bridge Enable

See the “Turn on IP Phone BIB to Allow Monitoring or Recording” section on page 34-64 for more information about this service parameter.

Related Topics

- Configuration Checklist for Monitoring and Recording, page 34-1
- Introducing Monitoring and Recording, page 34-2
- System Requirements for Monitoring and Recording, page 34-59
- Interactions and Limitations, page 34-60
- Configuring Monitoring and Recording, page 34-63
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Application User Configuration, Cisco Unified Communications Manager Administration Guide
- User Group Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Directory Number Configuration, Cisco Unified Communications Manager Administration Guide
- Recording Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Trunk Configuration, Cisco Unified Communications Manager Administration Guide
- External Call Control, page 22-1
Multilevel Precedence and Preemption

The Multilevel Precedence and Preemption (MLPP) service allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.

Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device.

An authenticated user can preempt calls either to targeted stations or through fully subscribed time-division-multiplexing (TDM) trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

This chapter covers the following topics:
- Configuration Checklist for MLPP, page 35-1
- Introducing MLPP, page 35-3
- MLPP Supplementary Services, page 35-33
- System Requirements for Multilevel Precedence and Preemption, page 35-38
- Devices That Support Multilevel Precedence and Preemption, page 35-38
- Interactions and Restrictions, page 35-39
- Installing and Activating MLPP, page 35-41
- Configuring MLPP, page 35-42
- Setting the Enterprise Parameters for MLPP, page 35-42
- Related Topics, page 35-43

Configuration Checklist for MLPP

The Multilevel Precedence and Preemption (MLPP) service allows properly validated users to place priority calls. If necessary, users can preempt lower priority phone calls.

Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device.
An authenticated user can preempt calls either to targeted stations or through fully subscribed time-division-multiplexing (TDM) trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as during a national emergency or degraded network situations.

Table 35-1 provides a checklist to configure MLPP. For more information on MLPP, see the “Introducing MLPP” section on page 35-3 and the “Related Topics” section on page 35-43.

Table 35-1 MLPP Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1                                                                flip. Configure MLPP Domains, Resource Priority Namespace Network Domain, and Resource Priority Namespace Network Domain List.</td>
<td>MLPP Domain Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Resource Priority Namespace Network Domain Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Resource Priority Namespace List Configuration Settings, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 2                                                                flip. Configure a common device configuration for which associated devices can make MLPP calls.</td>
<td>Device Pool Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 3                                                                flip. Set enterprise parameters to enable MLPP indication and preemption. If individual devices and devices in common device configurations have MLPP settings of Default, the MLLP-related enterprise parameters apply to these devices and common device configurations.</td>
<td>Setting the Enterprise Parameters for MLPP, page 35-42</td>
</tr>
<tr>
<td></td>
<td>Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 4                                                                flip. Configure partitions and Calling Search Spaces (CSS) that allow users (calling parties and their associated devices) to place precedence calls that use MLPP.</td>
<td>Partition Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 5                                                                flip. Configure route patterns/hunt pilots that specify MLPP precedence level and route options for MLPP calls.</td>
<td>Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td>Step 6                                                                flip. Configure translation patterns that specify MLPP precedence level and route options for MLPP calls.</td>
<td>Translation Pattern Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>
Introducing MLPP

The Multilevel Precedence and Preemption (MLPP) service allows placement of priority calls. Properly validated users can preempt lower priority phone calls with higher priority calls. An authenticated user can preempt calls either to targeted stations or through fully subscribed TDM trunks. This capability assures high-ranking personnel of communication to critical organizations and personnel during network stress situations, such as a national emergency or degraded network situations.

The following topics describe the MLPP service:

- **MLPP Terminology**, page 35-4
- **Precedence**, page 35-5
- **Executive Override Precedence Level**, page 35-6
- **Preemption**, page 35-8
- **Domain**, page 35-9

---

Table 35-1 MLPP Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Gateway Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configure gateways that specify an MLPP domain for MLPP calls. The following gateway types apply:</td>
</tr>
<tr>
<td></td>
<td>- Cisco Catalyst 6000 24 port FXS Gateway</td>
</tr>
<tr>
<td></td>
<td>- Cisco Catalyst 6000 E1 VoIP Gateway</td>
</tr>
<tr>
<td></td>
<td>- Cisco Catalyst 6000 T1 VoIP Gateway</td>
</tr>
<tr>
<td></td>
<td>- Cisco DE-30+ Gateway</td>
</tr>
<tr>
<td></td>
<td>- Cisco DT-24+ Gateway</td>
</tr>
<tr>
<td></td>
<td>- H.323 Gateway</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Some gateway types allow configuration of MLPP Indication and MLPP Preemption settings.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configure Cisco Unified IP Phones that specify an MLPP domain for MLPP calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Some phone types allow configuration of MLPP Indication and MLPP Preemption settings.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configure the directory number that will place an MLPP call.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Device Profile Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configure the User Device Profile of the user that will make an MLPP call.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Default Device Profile Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Configure the Device Profile Default for devices that will make MLPP calls.</td>
</tr>
<tr>
<td>Step 12</td>
<td>See the phone documentation for instructions on how users access MLPP features on their Cisco Unified IP Phone.</td>
</tr>
<tr>
<td></td>
<td>Notify users that the MLPP service is available.</td>
</tr>
</tbody>
</table>
MLPP Terminology

The following terms apply to the MLPP service:

- **Call**—A voice, video, or data connection between two or more users or network entities that is achieved by dialing digits or otherwise routing to a destination according to a predefined dialing plan.
- **Precedence**—Priority level that is associated with a call.
- **Preemption**—Process that terminates existing calls of lower precedence and extends a call of higher precedence to or through that target device.
- **Precedence call**—A call with precedence level that is higher than the lowest level of precedence.
- **MLPP call**—A call that has a precedence level established and is either being set up (that is, before alerting) or is set up.
- **Active call**—A call that has the connection established and the calling and called parties are active on the call.
• MLPP domain ID—Specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.

• Resource Priority Namespace Network Domain—Specifies SIP trunk behavior in the case of a precedence call and can preempt an existing call. The Resource Priority Namespace Network Domain in SIP signaling is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks. The Resource Priority Namespace Network Domain is included on outbound calls and based on translation patterns or route patterns directing the call to the SIP trunk. For incoming calls the network domain is validated against the Resource Priority Namespace Network Domain List. If the network domain is not on the list, the call is rejected and a 417 message (unrecognizable) is returned.


• MLPP Indication Enabled device—In Cisco Unified Communications Manager, a device for which the device and Cisco Unified Communications Manager support precedence and preemption signaling procedures in the device control protocol and that is configured as such in the Cisco Unified Communications Manager system.

• MLPP Preemption Enabled device—In Cisco Unified Communications Manager, a device for which the device and Cisco Unified Communications Manager support preemption signaling procedures in the device control protocol and that is configured as such in the Cisco Unified Communications Manager system. Cisco Unified Communications Manager can initiate preemption on this interface.

**Precedence**

Precedence indicates the priority level that is associated with a call. Precedence assignment represents an ad hoc action in that the user may choose to apply or not to apply a precedence level to a call attempt. MLPP precedence does not relate to call admission control or enhanced emergency services (E911). Dedicated dial patterns in Cisco Unified Communications Manager Administration allow users to initiate an MLPP request. Configuration of the calling search space(s) (CSS) that is associated with the calling party (device, line, and so forth) controls the ability of a calling party to dial a precedence pattern to attempt to originate a precedence call.

The Defense Switched Network (DSN) and the Defense Red Switched Network (DRSN) designate the target system for initial MLPP deployment. You generally can apply mechanisms for assigning precedence levels to calls, however, in Cisco Unified Communications Manager Administration to any dial plan by defining precedence dial patterns and calling search spaces that allow or restrict access to these patterns. In the DSN, a dial plan gets defined such that a precedence call is requested by using the string prefix NP, where P specifies the requested precedence level and N specifies the preconfigured MLPP access digit. Precedence priorities are as follows.

• Executive Override
• Flash Override
• Flash
• Immediate
• Priority
• Routine
Without specific invocation of precedence, the system processes a call by using normal call processing and call forwarding.

When a user profile is assigned to a phone, either as a default assignment or through extension mobility, the phone inherits the configuration of the assigned user, including any CSS that is associated with the user. The phone CSS can, however, override the user profile. Cisco Unified Communications Manager assigns the precedence level that is associated with the dialed pattern to the call when a pattern match occurs. The system sets the call request as a precedence call with the assigned precedence level.

When a precedence call is offered to a destination, Cisco Unified Communications Manager provides precedence indications to the source and destination of a precedence call, respectively, if either is MLPP Indication Enabled. For the source, this indication comprises a precedence ringback tone and display of the precedence level/domain of the call, if the device supports display. For the destination, the indication comprises a precedence ringer and display of the precedence level/domain of the call, if the device supports display.

Executive Override Precedence Level

The highest precedence level specifies the Executive Override precedence level. When the Executive Override precedence level preempts a lower precedence call, the Executive Override call can change its precedence level to Flash Override (next highest level), so a subsequent Executive Override call can preempt the first precedence call.

Preempting an Executive Override precedence call requires that the Executive Override Call Preemptable service parameter be set to True. If the service parameter is set to False, an Executive Override precedence call keeps its precedence level and cannot be preempted.

Figure 35-1 shows an example of two Executive Override precedence calls, one that can be preempted, and one that cannot be preempted.

![Figure 35-1 Executive Override Precedence Calls Example](image)

In the example, in Cisco Unified Communications Manager installation 1, the Executive Override Call Preemptable service parameter specifies False, whereas in Cisco Unified Communications Manager installation 2, the Executive Override Call Preemptable service parameter specifies True.

In the example, ONA makes an Executive Override precedence call to DNA from installation 1 to installation 2 through the T1 PRI 4ESS trunk. DNA answers, and the call connects.

In installation 1, if ONB tries to call ONA by placing an Executive Override precedence call, ONB receives a Blocked Precedence Announcement (BPA) because Executive Override calls cannot be preempted in installation 1. If ONB calls DNA by placing an Executive Override precedence call, the
call between ONA and DNA gets preempted because Executive Override calls can be preempted in installation 2. Likewise, if DNB calls DNA by placing an Executive Override precedence call, the subsequent Executive Override precedence call preempts the call between ONA and DNA.

**Executive Override Precedence Call Setup**

Figure 35-2 shows an example of the events that take place when an Executive Override precedence call gets placed.

*Figure 35-2  Executive Override Precedence Call Setup*

In the example, phone 1000 goes off hook and dials 9*1001. (Route pattern 9*XXXX setting specifies Executive Override.)

For the source, if this precedence call succeeds, Cisco Unified Communications Manager signals Cisco Unified IP Phone to play a ringback tone to the user. If Cisco Unified IP Phone 1000 is MLPP Indication Enabled, precedence ringback tone plays. Otherwise, normal ringback tone plays.

If the precedence call cannot connect, a Blocked Precedence Announcement (BPA) plays if Cisco Unified IP Phone 1000 is MLPP Indication Enabled. Otherwise, a normal reorder tone plays.

For the destination, if the Executive Override precedence call gets offered to Cisco Unified IP Phone 1001 successfully, Cisco Unified Communications Manager signals the destination to generate an audible ringer at the device. If Cisco Unified IP Phone 1001 is MLPP Indication Enabled, a precedence ring plays. Otherwise, a normal ring plays.

Also, Cisco Unified IP Phone 1001 displays precedence information (such as the Flash Override precedence call icon) if phone 1001 is MLPP Indication Enabled. Otherwise, no precedence information displays.
Executive Override Precedence Calls Across the PRI 4ESS Interface

Figure 35-3 shows an example of an Executive Override precedence call across the PRI 4ESS interface.

Cisco Unified Communications Manager processes Executive Override precedence calls across the PRI 4ESS interface by using the same method that it uses to process other precedence calls, except that the precedence level passes through PRI 4ESS UUIE.

The precedence information through UUIE gets passed only when User-to-User IE Status on the Service Parameter Configuration window is True and Passing Precedence Level Through UUIE gets selected on the Gateway Configuration window.

PRI 4ESS UUIE-Based MLPP Interface to DRSN

Cisco Unified Communications Manager now supports passing the MLPP information through the PRI 4ESS UUIE field. A previous release of Cisco Unified Communications Manager offered MLPP for PRI interface that was developed according to the ANSI T1.619a specification to connect with Defense Switched Network (DSN) switches. Defense Red Switch Network (DRSN) switches do not support ANSI T1.619a-based MLPP but do support MLPP over the PRI 4ESS interface by using the UUIE.

Preemption

The preemption process terminates lower precedence calls that are currently using the target device, so a call of higher precedence can be extended to or through the device. Preemption includes the notification and acknowledgement of preempted users and the reservation of shared resources immediately after preemption and prior to call termination. Preemption can take one of the following forms, depending on which method is invoked:

- User Access Channel Preemption—This type of preemption applies to phones and other end-user devices. In this type of preemption, if a called user access channel needs to be preempted, both the called party and the parties to which it is connected receive preemption notification, and the existing MLPP call gets cleared immediately. The called party must acknowledge the preemption before the higher precedence call completes. The called party then gets offered the new MLPP call. If the called party does not acknowledge the preemption, the higher precedence call does proceed after 30 seconds.
Common Network Facility Preemption—This type of preemption applies to trunks. This type of preemption means that the network resource is busy with calls, some of which are of lower precedence than the call that the calling party requests. One or more of these lower precedence calls gets preempted to complete the higher precedence call.

Ensure that all devices that a call uses to preempt an existing call are preemption enabled. Because it is not sufficient for the calling and called devices (phone) to be preemption enable, ensure that the gateways that are used for the call also are preemption enabled.

Domain

An MLPP domain specifies a collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher precedence call. MLPP service availability does not go across different domains.

The MLPP domain subscription of the originating user determines the domain of the call and its connections. Only higher precedence calls in one domain can preempt connections that calls in the same domain are using.

Administrators enter domains in Cisco Unified Communications Manager Administration as hexadecimal values of zero or greater.

Additional Information

See the “Related Topics” section on page 35-43.

Resource Priority Namespace Network Domain

The Resource Priority Namespace Network Domain enables the configuration of namespace domains for a Voice over Secured IP (VoSIP) network that uses SIP trunks. Cisco Unified Communications Manager prioritizes the SIP-signaled resources so that those resources can be used most effectively during emergencies and congestion of telephone circuits, IP bandwidth, and gateways. Endpoints receive the precedence and preemption information. It is based on RFC 4411 and RFC 4412.

The SIP signaling contains a resource-priority header. The resource-priority header is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks. The resource-priority header is related to, but is different from the priority header in RFC 3261, Section 20.26.

The RFC 3261 priority header indicates the importance of SIP requests for the endpoint. For example, the header could indicate decisions about call routing to mobile devices and assistants and about call acceptance when the call destination is busy. The RFC 3261 priority header does not affect the usage of PSTN gateway or proxy resources.

In the RFC 3261 priority header, any value could be asserted but the Resource Priority header field in the namespace network domain is subject to authorization. The Resource Priority header field does not directly influence the forwarding behavior of IP routers or the use of communications resources such as packet forwarding priority.
Chapter 35  Multilevel Precedence and Preemption

Introducing MLPP

The RFC 4411 and RFC 4412 resource-priority header in the outbound message is based on the translation or route patterns directing a call to the SIP trunk. Incoming calls are validated against a list of Resource Priority Namespace Network Domains if the calls are terminating to an endpoint configured in the Cisco Unified Communications Manager Administration.

The following messages include the Resource Priority header:

- INVITE
- UPDATE
- REFER

The following is an example of an INVITE message that has a resource priority header that specifies immediate priority (value of 4).

```
INVITE sip:6000@10.18.154.36:SIP/2.0Via: SIP/2.0/TCP 10.18.154.44;branch=z9hG4bK1636ee4aRemote-Party-ID: "Raleigh - 5001"
<sip:5001@10.18.154.44>;party=calling;screen=yes;privacy=offFrom: "Raleigh - 5001"
<sip:5001@10.18.154.44>;tag=936ad6ec-4d3c-4a42-a812-99ac56d972e1-14875646To:
<sip:6000@10.18.154.36>
```

You can also add a default Resource Priority Namespace Network Domain to a SIP Profile to use when handling misconfigured incoming namespace network domains.

---

Note

Digit analysis of translation and route patterns is supported.

The following supplementary services are supported:

- Precedence Call Waiting
- Call Transfer
- Call Forwarding
- Three-way Calling

The following headers, mapping, and queuing are not supported:

- Accept-Resource-Priority header.
- Inclusion of RP header in PRACK and ACK.
- Mapping of precedence levels between namespaces.
- Call queuing and other non-MLPP services.
Resource Priority Namespace Network Domain List

The Resource Priority Namespace Network Domain List contains acceptable network domains and is added to the SIP Profile. Incoming calls are compared to the list and processed if an acceptable network domain is in the list. If the incoming call is not valid, the call is rejected and an error response of 417 (Unknown) is sent to the calling party.

Location-Based MLPP

Cisco Unified Communications Manager supports MLPP on Skinny Client Control Protocol phones and TDM (PRI/CAS) trunks. Cisco Unified Communications Manager also supports MLPP on wide-area network (WAN) links. Location-based call admission control (CAC) manages WAN link bandwidth in Cisco Unified Communications Manager. Enhanced locations take into account the precedence level of calls and preempt calls of lower precedence when necessary to accommodate higher precedence calls.

Enhancing locations mean that, when a precedence call arrives and not enough bandwidth can be found to connect the call to the destination location, Cisco Unified Communications Manager finds the call or calls with the lowest precedence level and preempts the call(s) to make sufficient bandwidth available for a higher precedence call. If the bandwidth requirement still cannot be satisfied after going through the preemption procedure, the newly placed call fails.

Additional Information
See the “Related Topics” section on page 35-43.

MLPP Over Intercluster Trunks

Cisco Unified Communications Manager supports MLPP precedence and preemption over intercluster trunks. Dialed digits communicate the precedence level. The location call admission control mechanism controls preemption. Announcements and MLPP cause codes also become available across intercluster trunks.

MLPP Precedence Patterns

To set up MLPP precedence patterns, access the Translation Pattern Configuration window in Cisco Unified Communications Manager Administration where the following MLPP precedence patterns are available:

- Executive override (highest)
- Flash override
- Flash
- Immediate
- Priority
- Routine (lowest)
- Default (means precedence level does not get changed)
Introducing MLPP

See the Translation Pattern Configuration section in the Cisco Unified Communications Manager Administration Guide for details.

MLPP Indication Enabled

MLPP indication-enabled devices include the following characteristics:

- MLPP indication-enabled devices can play preemption tones.
- MLPP indication-enabled devices can receive MLPP preemption announcements that the announcement server generates.
- MLPP indication-enabled devices can receive preemption.

To set up devices to enable MLPP indication, use the configuration window for each respective device. In the MLPP Indication field of each device, set the value to On.

See the following topics for details of setting MLPP indication for devices:

- Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Default Device Profile Configuration, Cisco Unified Communications Manager Administration Guide

Precedence Call Setup

The following sequence of events takes place during setup of a precedence call:

1. User goes off hook and dials a precedence call. The call pattern specifies NP-XXX, where N specifies the precedence access digit and P specifies the precedence level for the call.
2. The calling party receives the special precedence ringback and a precedence display while the call is processing.
3. The called party receives the special precedence ringer and a precedence display that indicates the precedence call.

Example

Party 1000 makes a precedence call to party 1001. To do so, party 1000 dials the precedence call pattern, such as 90-1001.

While the call processes, the calling party receives precedence ringback and precedence display on the calling Cisco Unified IP Phone. After acknowledging the precedence call, the called party receives a precedence ringer (receives a special ring) and a precedence display on the called Cisco Unified IP Phone.
**Precedence Call Setup Across Intercluster Trunks**

Figure 35-4 shows an example of a configuration that can be used to set up precedence calls over intercluster trunks. Because no precedence information element support exists over intercluster trunks, transmission of extra digits carries the precedence information. The dial plan must be set up appropriately on both clusters to accomplish transmission of the precedence information.

**Figure 35-4  Precedence Call Setup Across Intercluster Trunks Example**

In this example, 1000 dials 92-2000, which matches the appropriate precedence patterns on both clusters and sets up the precedence call.

**Alternate Party Diversion**

Alternate Party Diversion (APD) comprises a special type of call forwarding. If users are configured for APD, APD takes place when a precedence call is directed to a directory number (DN) that is busy or does not answer.

MLPP APD applies only to precedence calls. An MLPP APD call disables the DN Call Forward No Answer setting for precedence calls.

Precedence calls do not normally forward to voice-messaging system, as controlled by the value of the Use Standard VM Handling For Precedence Calls enterprise parameter. See the “Setting the Enterprise Parameters for MLPP” section on page 35-42 for details.

To set up APD, the administrator configures the Multilevel Precedence and Preemption Alternate Party Settings on the Directory Number Configuration window of the DN that is the target of an MLPP precedence call. See the Cisco Unified IP Phone Configuration section of the Cisco Unified Communications Manager Administration Guide for details.
Example

Figure 35-5 illustrates the Alternate Party Diversion that takes place when a called party receives a precedence call and the party is configured for Alternate Party Diversion.

Figure 35-5 Alternate Party Diversion Example

In the example, a calling party placed a precedence call to party 1000. Called party 1000 has a Call Forward Busy (CFB) setting of 2000 and a Call Forward Alternate Party (CFAP) setting of 1001. The figure shows the CFB and CFAP settings for all other parties in this example.

When 1000 receives a precedence call but is busy, the call routes to party 2000. If party 2000 is also busy, the call routes to party 3000. If neither party 2000 nor party 3000 answers the call, however, the call routes to party 1001. That is, the call routes to the alternate party that is designated for the originally called party, not to the alternate parties that are designated for the Call Forward Busy parties that are associated with the originally called party.

Likewise, if party 1001 is busy and does not answer the call, the call forwards to party 5000. If party 5000 is busy, the call forwards to party 6000. If neither party 5000 nor party 6000 answers the call, however, the call forwards to the alternate party destination of party 1001, which is party 1002. If party 1002 is busy or does not answer, the call forwards to party 1003, which is the alternate party designation of party 1002.
**MLPP Preemption Enabled**

Enable MLPP preemption by explicitly configuring preemption-capable devices for preemption.

**Receiving Preemption**

A device that is preemption disabled (by setting the MLPP Preemption value to Disabled) can still receive precedence calls in an MLPP network, but the device itself does not get preempted. The preemption-disabled device can be connected to a call that gets preempted (at another device), in which case, the device receives preemption.

**Preemption Enabled**

Enable devices for preemption by setting the device MLPP Preemption value to either Forceful or Default. If the device MLPP Preemption value is set to Forceful, the system can preempt the device at its own interface. That is, the device can get preempted when a precedence call contends for the device resources.

If the device MLPP Preemption setting is Default, the device inherits its MLPP Preemption setting from its common device configuration. If the common device configuration MLPP Preemption setting for the device is Forceful, or if the common device configuration MLPP Preemption setting is also Default but the MLPP Preemption Setting enterprise parameter value is Forceful Preemption, the device inherits preemption enabling.

To set up devices to enable MLPP preemption, use the configuration window for each respective device. In the MLPP Preemption field of each device, set the value to Forceful or Default.

See the following topics for details of setting MLPP preemption for devices:
- Common Device Configuration, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Default Device Profile Configuration, Cisco Unified Communications Manager Administration Guide

**Preemption Details**

The following types of preemption exist:
- User Access Preemption
- Common Network Facility Preemption
- Location-based Preemption

**User Access Preemption**

User access preemption takes place when a user places a precedence call to a user that is already active on a lower level precedence call. Both calls exist in the same MLPP domain. You can use this type of preemption for MLPP Indication Enabled phones that the Cisco Skinny Client Control Protocol controls.
Introducing MLPP

in the Cisco Unified Communications Manager MLPP system. Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call that is connected at the destination MLPP Preemption Enabled phone. Call processing uses a preemption tone to notify the connected parties of the preemption and releases the active call. When the called party acknowledges the preemption by hanging up, the called party gets offered the new MLPP call.

To understand the sequence of steps that takes place during user access preemption, see the following example.

**Example**

Figure 35-6 illustrates an example of user access preemption.

**Figure 35-6 User Access Preemption Example**

In the example of user access preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level flash override to user 1001, who answers the call. In this example, user 1000 dials 90-1001 to place the precedence call.

2. User 1002 places a precedence call to user 1001 by dialing 9*-1001. This call, which is of precedence level Executive Override, represents a higher precedence call than the active precedence call.

3. While the call is directed to user 1001, the calling party receives precedence display (that is, flash override display, not executive override display), and the parties who are involved in the existing lower precedence call both receive preemption tones.

4. To complete preemption, the parties who are involved in the lower precedence call (users 1000 and 1001) hang up.

5. The higher level precedence call gets offered to user 1001, who receives a precedence ringer. The calling party, user 1002, receives precedence ringback.

Distinct preemption types take place in this instance. For the party that is not the destination of the higher precedence call, Preemption Not for Reuse takes place. Because preemption is not taking place at this interface, this device does not need to be preemption enabled. For the party that is the destination of the higher precedence call, Preemption for Reuse takes place. Because preemption does take place at this interface, ensure that this device is preemption enabled.
User Access Channel Nonpreemptable

You can configure an end-user device as MLPP Indication Enabled but not MLPP Preemption Enabled. In this case, a phone that can generate MLPP indications (using special preemption tones and ringers) does not have preemption procedures that are supported in its device control protocol in Cisco Unified Communications Manager. The administrator can also disable preemption procedures for a phone even though Cisco Unified Communications Manager Administration supports the procedures.

Historically, user access devices (phones) have limited or no mechanisms for handling multiple, simultaneous calls. Even with the Call Waiting feature, many phones and associated switches do not have a mechanism to allow the user to manage multiple calls simultaneously on the same line.

Cisco Unified Communications Manager Administration effectively enhances the Call Waiting feature to provide this capability for users of Cisco Unified IP Phones 7940, 7942, 7945, 7960, 7962, 7965, and 7975. These Cisco Unified IP Phones include a user interface that gives the user adequate control of multiple, simultaneous calls when interfacing with the Cisco Unified Communications Manager system. This enhanced functionality allows the Call Waiting feature to be applied to all precedence calls that are directed to these types of phones, even though the user may already be managing other calls. When the user receives a precedence call, the user at a destination phone can decide what to do with any existing calls instead of merely releasing the lower precedence call. For users of these devices, the Cisco Unified Communications Manager administrator can configure devices as not MLPP Preemption Enabled to take advantage of this function in Cisco Unified Communications Manager.

Common Network Facility Preemption

Common network facility preemption applies to network resources, such as trunks, in the MLPP system. When a common network facility gets preempted, all existing parties receive notification of the preemption, and the existing connection immediately gets disconnected. The new call gets set up by using the preempted facility in the normal manner without any special notification to the new called party. PRI and T1-CAS trunks on targeted MGCP gateway platforms support this type of preemption in Cisco Unified Communications Manager.

Preemption occurs if a precedence call request is validated and if the requested precedence of the call is greater than the precedence of an existing call through the destination MLPP Preemption Enabled trunk and the trunk is completely busy (that is, cannot handle any more calls). Call processing identifies a call with lower precedence, notifies the connected parties of the preemption for the PRI trunk interface, reserves the channel for subsequent use, and drops the selected lower precedence call. The system uses the reserved channel to establish the connection through the gateway for the precedence call that caused preemption.

For the sequence of steps that takes place during common network facility preemption, see the following examples.
Example 1

Figure 35-7 illustrates an example of common network facility preemption.

Figure 35-7  Common Network Facility Preemption Example

In the example of common network facility preemption, the following sequence of events takes place:

1. User 1000 places a precedence call of precedence level Flash Override to user 2000, who answers the call. In this example, user 1000 dials 90-2000 to place the precedence call. The flash call of precedence level Flash Override specifies active.

   The call uses a common network facility where the two gateways define a fully subscribed TDM trunk.

2. User 1001 next places a higher precedence (executive override) call to user 2001 by dialing *9-2001. (Assume that the flash call represents the lowest precedence call over gateway A, and users 1000 and 1001 reside in the same MLPP domain.)

   Preemption occurs at gateway A, which is preempted for reuse. Because preemption occurs at this interface, you must ensure that this device is preemption enabled. Gateway B also gets preempted for reuse, but the preemption does not occur at this interface, so this device does not need to be preemption enabled.

   Users 1000 and 2000 both receive preemption tones. Because both devices are not preempted for reuse and preemption does not occur at these interfaces, you do not need to ensure that these devices are preemption enabled for the preemption to occur.

In this example, almost all events occur instantly. Parties do not need to hang up for common network facility preemption to occur.
Example 2

Figure 35-8 illustrates an example of common network facility preemption with the retry timer Trr. The retry timer Trr provides a mechanism, so if preemption is not successful on one channel, preemption gets retried on another channel. This timer applies only to TDM trunks.

Figure 35-8 Common Network Facility Preemption Example with Retry Timer Trr

In the example of common network facility preemption with the retry timer Trr, the following sequence of events takes place:

1. An incoming call with Flash Override precedence arrives at a PRI trunk device.
   
   The incoming call causes preemption of channel 3, but a response does not occur within the time that the retry timer Trr specifies.

2. Retry timer Trr expires.
   
   Channel 3 gets preempted.

3. This preemption causes a response, and the precedence call gets offered on channel 1.

Location-Based Preemption

The following examples illustrate location-based preemption.

Example 1

In the example that follows, the new call and the location-preempted call take place in different devices. See Figure 35-9 for an example of this type of location-based preemption.
This example illustrates the location-based preemption scenario. In the example, three locations exist:

- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phones B and C and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

The following sequence of events takes place:

1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls C with Immediate precedence level. The D call preempts the call between A and B because RL1 is out of bandwidth and D call has higher precedence.
3. The call between D and C completes. The available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.
Example 2
In the example that follows, the new call and the location preempted call take place in the same device. See Figure 35-10 for an example of this type of location-based preemption.

Figure 35-10 Location-Based Preemption in the Same Device

This example illustrates the location-based preemption scenario. In the example, three locations exist:
- Remote location 0 (RL0) with phone A and 160K of available bandwidth
- Remote location 1 (RL1) with phone B and 80K of available bandwidth
- Remote location 2 (RL2) with phone D and 240K of available bandwidth

The following sequence of events takes place:
1. A places a call to B with Priority precedence level, and the call becomes active. The available bandwidth specifies 80K in RL0, 0K in RL1, and 240K in RL2.
2. D calls B with Immediate precedence level. D call preempts the call between A and B because RL1 is out of bandwidth and D call has higher precedence.
3. B receives the preemption tone first, and the End call softkey displays.
4. B presses the EndCall softkey, hangs up, or waits for timeout. The call from D to B gets offered to B. When the call from D to B completes, the available bandwidth specifies 160K in RL0, 0K in RL1, and 160K in RL2.

Figure 35-11

MLPP Announcements
Users who unsuccessfully attempt to place MLPP precedence calls receive various announcements that detail the reasons why a precedence call was blocked.
The following sections discuss specific MLPP announcements:

- Unauthorized Precedence Announcement, page 35-22
- Blocked Precedence Announcement, page 35-23
- Busy Station Not Equipped for Preemption, page 35-24
- Announcements Over Intercluster Trunks, page 35-24

The Supported Tones and Announcements topic in the “Annunciator” chapter of the Cisco Unified Communications Manager System Guide discusses MLPP announcements. See the Route Pattern Configuration and Translation Pattern Configuration sections in the Cisco Unified Communications Manager Administration Guide for details of configuring the Precedence Level Exceeded condition that generates the Unauthorized Precedence Announcement.

Additional Information
See the “Related Topics” section on page 35-43.

Unauthorized Precedence Announcement

Users receive an unauthorized precedence announcement when they attempt to make a call with a higher level of precedence than the highest precedence level that is authorized for their line. A user receives an unauthorized precedence announcement when the user dials a precedence call by using a calling pattern for which the user does not have authorization.

Cisco Unified Communications Manager recognizes the Precedence Level Exceeded condition only if specific patterns or partitions are configured to block a call attempt that matches the pattern and that indicates the reason that the call is blocked.

To assign authorized calling patterns, access the Route Pattern/Hunt Pilot Configuration and the Translation Pattern Configuration windows in Cisco Unified Communications Manager Administration. To configure the MLPP Precedence Level Exceeded condition, use the Route Option field of the Route Pattern/Hunt Pilot Configuration and Translation Pattern Configuration windows and choose the Block this pattern option in Cisco Unified Communications Manager Administration. In the drop-down list box, choose Precedence Level Exceeded. See the Route Pattern Configuration and Translation Pattern Configuration sections of the Cisco Unified Communications Manager Administration Guide for details.
Example

Figure 35-12 illustrates an example of a user that receives an unauthorized precedence announcement.

Figure 35-12 Unauthorized Precedence Announcement Example

In the example, user 1002 dials 90 to start a precedence call. Nine (9) represents the precedence access digit, and zero (0) specifies the precedence level that the user attempts to use. Because this user is not authorized to make flash override precedence calls (calls of precedence level 0), the user receives an unauthorized precedence announcement.

Blocked Precedence Announcement

Users receive a blocked precedence announcement if the destination party for the precedence call is off hook, or if the destination party is busy with a precedence call of an equal or higher precedence and the destination party does not have the Call Waiting nor Call Forward features nor a designated party for alternate party diversion (APD), or due to a lack of a common network resource.

Example

Figure 35-13 provides an example of a blocked precedence announcement.

Figure 35-13 Blocked Precedence Announcement Example
In this example, user 1000 makes a precedence call to user 1001 by dialing 90-1001. Because user 1001 is either off hook or busy with a precedence call of equal or higher precedence level and user 1001 does not have Call Waiting nor Call Forward nor an alternate party that is designed for alternate party diversion, user 1000 receives a blocked precedence announcement.

**Busy Station Not Equipped for Preemption**

Users receive this announcement if the dialed number is nonpreemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations.

**Announcements Over Intercluster Trunks**

Figure 35-14 illustrates an instance of an MLPP announcement that is streamed over an intercluster trunk.

In the example, phones 1000 and 2000 reside on two clusters that an intercluster trunk connects. User 2000 does not have features such as calling waiting and call forwarding configured.

The following sequence of events takes place:

1. User 2000 goes off hook and starts to dial. (Status for User 2000 specifies originating busy and not preemptable.)
2. User 1000 then dials a precedence call over the intercluster trunk to user 2000. Because user 2000 is busy and is not preemptable, the call gets rejected.
3. Because user 1000 originated a precedence call, the call receives precedence treatment, and the announcement server on the remote cluster streams the appropriate Blocked Precedence Announcement (BPA) to 1000 with the switch name and the location of the cluster.
MLPP Numbering Plan Access Control for Precedence Patterns

MLPP uses the calling search spaces and partitions that are defined for users to authenticate and validate MLPP calls and provide access control for precedence patterns.

The maximum precedence of a user gets set at user configuration time. All MLPP-capable station devices get configured as either MLPP-enabled or MLPP-disabled. A device to which a user profile is applied inherits the precedence level of that user with respect to precedence calls that are initiated from that device. A device that has a default user assigned inherits a Routine precedence level for the default user.

Configuration of the calling search space(s) (CSS) that is associated with the calling party controls ability of a user to dial a precedence pattern (that is, to initiate a precedence call). Cisco Unified Communications Manager does not provide for explicit configuration of an explicit maximum allowed precedence value.

The following example illustrates the differences in access to precedence calls for two users who try to place a priority-level precedence call to a third user.

Example

Figure 35-15 provides an example of MLPP numbering plan access control for precedence patterns.
The table defines three users in this illustration:

<table>
<thead>
<tr>
<th>User</th>
<th>Directory Number (DN)</th>
<th>Partition</th>
<th>Calling Search Space (CSS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>1000</td>
<td>Routine</td>
<td>Flash Override</td>
</tr>
<tr>
<td>Major</td>
<td>2000</td>
<td>Routine</td>
<td>Priority</td>
</tr>
<tr>
<td>Private</td>
<td>3000</td>
<td>Routine</td>
<td>Routine</td>
</tr>
</tbody>
</table>

The example shows the use of partitions and calling search spaces to limit access to precedence calls.
If private 3000 tries to place a precedence call by dialing the precedence pattern 93, the following events take place:
- Call processing searches for calling search space for private 3000, which is the Routine CSS.
- Within Routine CSS of private 3000, call processing finds the Block Priority partition.
- In the Block Priority partition, call processing finds the pattern 93 and goes to translation pattern 93.
- Translation pattern 93 determines that priority calls are blocked for this user (DN), and call processing issues an unauthorized precedence announcement (UPA).

If major 2000 places a precedence call by dialing the digits 931000, the following events take place:
- Call processing searches for calling search space for major 2000, which is the Priority CSS.
- Within Priority CSS for major 2000, call processing finds the Priority partition.
- In the Priority partition, call processing finds the pattern 93.XXXX and goes to translation pattern 93.XXXX.
- Translation pattern 93.XXXX determines that priority calls are authorized for this user (DN). Call processing therefore completes the Priority-level precedence call to user 1000, the general.

**MLPP Trunk Selection**

MLPP trunk selection entails hunting for available trunks by using route lists and route groups. In Cisco Unified Communications Manager Administration, you can configure a route list and associated route group(s) to route calls to several gateways via a single dial pattern to find an available channel. Although a route list has many trunk resources to which the route list can route calls, the individual resources may spread across many gateways.

When no available trunk resource is identified in a collection of gateways (that is, a route list and route group configuration), Cisco Unified Communications Manager attempts to initiate preemption of a lower level precedence shared resource in the collection. Two methods exist for subsequently searching for a preemptable channel within a route list and route group configuration.

**Method 1**

Configure a route list and a single route group. Add trunk interfaces (gateways) to the route group and position the Direct Route gateway as the first gateway in the route group. Associate the route group with the route list and choose the Top Down distribution algorithm. With this configuration, the system searches all gateways in the route group for an idle channel first. If no idle channel is found in any gateway in the route group, preemptive trunk selection begins with the first gateway in the route group (that is, the Direct Route gateway) as follows:

- Call processing chooses a current route from the collection on the basis of the distribution algorithm and offers the call to this gateway device to determine whether the gateway device can initiate preemption.
If the current gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), call processing chooses the next gateway in the collection as the current route and continues this sequence until a gateway device initiates preemption or until all gateway devices in the route list and route group collection have been searched.

**Method 2**

Configure a route list and a separate route group for each available route (trunk interface). Designate one route group as the Direct route group and designate the other route groups as Alternate route groups. Add the Direct Route trunk interface (gateway) as the only member of the Direct route group. Add the Alternate Route gateways to the individual Alternate route groups. Associate the route groups with the route list, configuring the Direct route group as the first route group in the route list, and choose the Top Down distribution algorithm for each route group association.

Using this configuration, the Direct gateway in the Direct route group gets searched for an idle channel first. If no idle channel is found in the Direct gateway, the system initiates preemptive trunk selection for this Direct gateway as follows:

- Call processing chooses the Direct route and offers the call to this gateway device to determine whether the gateway device can initiate preemption.
- If the Direct gateway device rejects the precedence call request (that is, the gateway device cannot initiate preemption), choose the next route group in the route list as the current route. Continue this sequence until an idle channel is found on the current gateway, or until the current gateway device has initiated preemption, or until all gateway devices in the route list and route group collection are searched.

**Example**

The following example illustrates two methods for finding an available trunk device when an incoming flash-level precedence call seeks an available trunk device.
Introducing MLPP

Figure 35-16 provides an example of MLPP trunk selection that uses route lists and route groups to hunt for an available trunk device.

**Figure 35-16  MLPP Trunk Selection (Hunting) Example**

In Method 1, the following sequence of events takes place:

1. An incoming flash-level precedence call reaches route list RL, which contains only one route group, RG1.
2. Route group RG1 contains three trunk devices.
   - Of the three trunk devices in RG1, Trunk Device1 and Trunk Device2 register as busy, so the system offers the call to Trunk Device3, which is available.

In Method 2, the following sequence of events takes place:

1. An incoming flash-level precedence call reaches route list RL and first goes to route group RG1, which directs the call to Trunk Device1, which is busy.
   - For Trunk Device1, calls must have a higher precedence than flash to preempt calls that are using this device.
2. The call therefore seeks the next route group in route list RL, which is route group RG2. Route group RG2 contains Trunk Device2, which is also busy, but precedence calls of a precedence level higher than Priority can preempt Trunk Device2.
   - Because this call is a higher precedence call, the call preempts the existing call on Trunk Device2.
MLPP Hierarchical Configuration

MLPP settings for devices follow this hierarchy:

- If MLPP Indication for a device is set to Off, the device cannot send indication of MLPP calls. If the device MLPP Preemption is set to Disabled, the device cannot preempt calls. These settings override the common device configuration settings for the device.

- If MLPP Indication for a device is set to On, the device can send indication of MLPP calls. If the MLPP Preemption for the device is set to Forceful, the device can preempt calls. These settings override the common device configuration settings for the device.

- If MLPP Indication for a device is set to Default, the device inherits its ability to send indication of MLPP calls from the common device configuration for the device. If the MLPP Preemption for a device is set to Default, the device inherits its ability to preempt calls from the common device configuration for the device.

MLPP settings for common device configurations follow this hierarchy:

- If a common device configuration MLPP Indication is set to Off, devices in the common device configuration cannot send indication of MLPP calls. If the common device configuration MLPP Preemption is set to Disabled, devices in the common device configuration cannot preempt calls. These settings override the MLPP enterprise parameter settings.

- If a common device configuration MLPP Indication is set to On, devices in the common device configuration can send indication of MLPP calls. If the common device configuration MLPP Preemption is set to Forceful, devices in the common device configuration can preempt calls. These settings override the MLPP enterprise parameter settings.

- If a common device configuration MLPP Indication is set to Default, the device inherits its ability to send indication of MLPP calls from the MLPP Indication Status enterprise parameter. If the common device configuration MLPP Preemption is set to Default, the common device configuration inherits its ability to preempt calls from the MLPP Preemption Setting enterprise parameter.

The MLPP Indication Status enterprise parameter defines the indication status of common device configurations and common device configurations in the enterprise, but nondefault settings for common device configurations and individual devices can override its value. The default value for this enterprise parameter specifies MLPP Indication turned off.

The MLPP Preemption Setting enterprise parameter defines the preemption ability for common device configurations and devices in the enterprise, but nondefault settings for common device configurations and individual devices can override its value. The default value for this enterprise parameter specifies No preemption allowed.

The MLPP Domain Identifier enterprise parameter specifies the MLPP domain. The MLPP service applies only to a domain; that is, only to the subscribers and the network and access resources that belong to a particular domain. Connections and resources that belong to a call from an MLPP subscriber get marked with a precedence level and an MLPP domain identifier. Only calls of higher precedence from MLPP users in the same domain can preempt lower precedence calls in the same domain.

Service Parameter Special Trace Configuration

MLPP issues a service parameter for tracing.

See the Cisco Unified Serviceability Administration Guide for details.
CDR Recording for Precedence Calls

MLPP precedence calls generate call detail records (CDRs). The CDR identifies the precedence level of the precedence call.

The same precedence levels of the call legs generally apply. With transfer or conference calls, the precedence levels can differ; therefore, Cisco Unified Communications Manager CDRs identify the precedence level of each leg of the call.

Cisco Unified Communications Manager CDRs document the preemption value for preempted call terminations.

See the Cisco Unified Serviceability Administration Guide for details.

Line Feature Interaction

MLPP interacts with line features as described in the following sections:

- Call Forward, page 35-30
- Call Transfer, page 35-31
- Shared Lines, page 35-31
- Call Waiting, page 35-31

Call Forward

MLPP interacts with the call forward features as described in the following list:

- Call Forward Busy
  - You optionally can configure a preconfigured Precedence Alternate Party target for any MLPP-enabled station.
  - Cisco Unified Communications Manager applies the Call Forward Busy feature to forward a precedence call in the usual manner prior to applying any Precedence Alternate Party Diversion procedures to the call.
  - If the incoming precedence call is of equal or lower precedence than the existing call, call processing invokes normal call-forwarding behavior.
  - If the destination station for a precedence call is nonpreemptable (that is, not MLPP-configured), call processing invokes call-forwarding behavior.
  - The system preserves precedence of calls across multiple forwarded calls.
  - If the incoming precedence call is of higher precedence than the existing call, preemption occurs. Both the preempted parties in the active call receive a continuous preemption tone until the station to which the precedence call is directed hangs up. After hanging up, the station to which the precedence call is directed receives precedence ringing. The destination station connects to the preempting call when the station goes off hook.

- Call Forward No Answer
  - For calls of Priority precedence level and above, call processing preserves the precedence level of calls during the forwarding process and may preempt the forwarded-to user.
  - If an Alternate Party is configured for the destination of a precedence call, call processing diverts the precedence call to the Alternate Party after the Precedence Call Alternate Party timeout expires.
If no Alternate Party setting is configured for the destination of a precedence call, call processing diverts the precedence call to the Call Forward No Answer setting.

- Normally, precedence calls route to users and not to the voice-messaging system. The administrator sets the Use Standard VM Handling For Precedence Calls enterprise parameter to avoid routing precedence calls to voice-messaging systems. See the “Setting the Enterprise Parameters for MLPP” section on page 35-42 for details.

### Call Transfer

MLPP interacts with the call-transfer feature. For blind transfers and consult transfers, each connection of the transferred call, including the consult call, maintains the precedence that the connection was assigned when the call was established.

### Shared Lines

MLPP interacts with shared lines. A shared-line appearance with a call on hold may be preempted to establish a higher precedence call to another terminal with the same directory number (DN). In this case, the original held call does not disconnect, and the precedence call connects. After the precedence call ends, the user may retrieve the original held call.

### Call Waiting

MLPP interacts with the call-waiting feature as described in the following list:

- When conflicts arise between call-waiting status and MLPP precedence calls due to the lack of network resources, the call gets preempted.
- When a precedence call is offered to a destination station that is configured with call waiting, the following behaviors take place:
  - If the requested precedence is higher than the existing call precedence, the existing call gets preempted. If the destination user is nonpreemptable, call processing invokes normal call-waiting behavior and alerting. If the precedence call is of Priority precedence level or higher, the destination user receives precedence call-waiting tones and cadences.
  - If the requested precedence level is the same as the existing call precedence, call processing invokes normal call-waiting behavior. If the precedence call is of Routine precedence, call processing alerts the destination with standard call-waiting tones. If the precedence call is of Priority or higher precedence, call processing alerts the destination with precedence call-waiting tones.
  - If the requested precedence level is lower than the existing call precedence, call processing invokes normal call-waiting behavior. If the precedence call is of Routine precedence, call processing alerts the destination with standard call-waiting tones. If the precedence call is of Priority or higher precedence, call processing alerts the destination with precedence call-waiting tones.
  - When a device has more than one appearance, the destination user may place a lower precedence call on hold to acknowledge receipt of a higher precedence call. After the higher precedence call ends, the destination user may resume the held, lower precedence call.
### Call Preservation

Any MGCP trunk call or connection that is preserved according to the Cisco Unified Communications Manager Call Preservation feature preserves its precedence level and MLPP domain after invoking the Call Preservation feature. After the device registers with Cisco Unified Communications Manager, the system only preserves the preserved calls at the device layer in the Cisco Unified Communications Manager system. As a result, the preserved calls get treated as two disjointed half calls. If preemption does occur on these devices, only one leg can follow preemption protocol to the other leg. The system detects call termination only through closure of the RTP port.

### Automated Alternate Routing

The Automated Alternate Routing (AAR) for Insufficient Bandwidth feature, an extension of AAR, provides a mechanism to automatically fall back to reroute a call through the Public Switched Telephone Network (PSTN) or other network by using an alternate number when the Cisco Unified Communications Manager blocks the call due to insufficient location bandwidth. With this feature, the caller does not need to hang up and redial the called party.

If a precedence call attempt meets a condition that invokes the AAR service, the precedence call gets rerouted through the PSTN or other network as specified by the AAR configuration. Cisco Unified Communications Manager handles the precedence nature of the call in the same manner as if the call originally had been routed through the PSTN or other network, based on the MLPP Indication Enabled and MLPP Preemption Enabled nature of the network interface through which the call is routed.

For details of configuring Automated Alternate Routing, see the Automated Alternate Routing Group Configuration section of the Cisco Unified Communications Manager Administration Guide.

### MGCP and PRI Protocol

MLPP supports Common Network Facility Preemption only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco Unified Communications Manager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

### Secure Endpoints and Secure Communications

The traditional Department of Defense (DOD) TDM network uses legacy analog secure telephone units (STUs) and BRI secure telephone equipment (STEs) as secure endpoints, which are critical for secure communication. The newly developed IP STE also requires support to reduce the need for legacy equipment. Cisco Unified Communications Manager supports the Skinny Client Control Protocol for these devices. Modem relay provides secure communication and uses the V.150 protocol.

### Mapping MLPP Precedence to DSCP Values

Cisco Unified Communications Manager maps the MLPP precedence levels to the DSCP values in the ToS field of the IP Header to prioritize calls in an IP network. You can map the following precedence levels to DSCP values:

- Executive Override
- Flash Override
You must map the MLPP precedence levels to the DSCP values identically for every Cisco Unified Communications Manager cluster within your network.

To map MLPP precedence levels to DSCP values, choose the DSCP value that you want mapped to each precedence level in the Clusterwide Parameters (System-QoS) section of the service parameters. Click the Save button to save the changes.

**MLPP Supplementary Services**

Cisco Unified Communications Manager Administration provides support for the following MLPP supplementary services and entities:

- MLPP Support for Multiple Appearance Lines, page 35-33
- Call Forwarding, page 35-34
- Three-Way Calling, page 35-35
- Call Transfer, page 35-35
- Call Pickup, page 35-36
- Hunt Pilots and Hunt Lists, page 35-36
- Supplementary Services Support for SCCP Gateway Endpoints, page 35-37

The subsections that follow discuss each MLPP supplementary service. For each supplementary service, the discussion provides a description, configuration information and recommendations, and troubleshooting information.

**MLPP Support for Multiple Appearance Lines**

If an empty call appearance is available and the busy trigger is not exceeded, an incoming precedence call gets presented such that the active line receives the precedence call-waiting tone and the endpoint display shows the appropriate precedence bubbles. The incoming call does not cause precedence ringing. Instead, precedence call-waiting tone occurs on the active appearance.

If no empty call appearances are available and the called endpoint does not have call forwarding configured, a higher precedence inbound call will preempt a lower active or nonactive call appearance on the endpoint. In the case of a tie, the active appearance gets preempted.

If a nonactive (held) appearance gets preempted, the incoming call shows the appropriate precedence bubbles on the endpoint display, and the precedence call-waiting tone gets presented on the active call appearance. The other preempted user (the other end of the held call) receives call preemption tone.

If the active call appearance gets preempted, normal call preemption takes place (preemption tone gets presented on the active appearance and on the other party active line). Any existing, nonactive (held) call appearances remain unaffected and can be picked up at any time.
Configuration
For MLPP support for multiple appearance lines to function correctly, Cisco recommends the following configuration:

- Cisco recommends, but does not require, setting IP phones with max calls=4 and busy trigger=2.
- When interaction with MLPP supplementary services occurs, no support exists for assigning the same DN twice to the same station by using multiple partitions.
- Disable the Auto Line Select option for all IP phones because the highest precedence call may not get answered when multiple alerting calls are incoming.

Troubleshooting
If you use the CCM trace log (with detailed trace configured), you can tell how the preemption criteria was applied on any inbound call by searching for the whatToDo tag.

Call Forwarding

The Department of Defense (DoD) requires that no precedence calls get forwarded to off-net endpoints, such as mobile phones. Additionally, forwarded calls must retain the original precedence across multiple forwarding hops.

For Call Forward All (CFA) scenarios, precedence calls get routed to the MLPP Alternate Party (MAP) target of the original called party immediately. The CFA target does not get used for MLPP calls.

For Call Forward Busy (CFB) scenarios, precedence calls get forwarded to the configured CFB destination, subject to the hop count limits described in the “Restrictions” section on page 35-40 and the state of open appearances on the called party endpoint.

For the Call Forward No Answer (CFNA) scenario, call processing attempts a single forward attempt (hop) to the CFNA target of the original called party. If that endpoint does not answer prior to the expiration of the No Answer timer, the call gets sent to the MAP target of the original called party.

Configuration
MLPP operation in the DoD requires that all MLPP endpoints have an MLPP Alternate Party (MAP) target directory number that is configured. The MAP typically specifies the attendant number and is used as a destination of last resort for forwarded MLPP calls.

If the endpoint does not follow the prescribed configuration when a MAP is needed, the MLPP call originator receives reorder tone, which indicates that the called party configuration does not include the required MAP configuration. This tone plays only if the call would have been directed to the attendant when no other forwarding options were available or configured.

Example
The following example describes a forwarding case. First, the MLPP call rings (3001 calls 3003 at Flash Override precedence level) with the CFNA timer set to 5 seconds. After the timer expires, the call gets redirected to the original called party CFNA target, which is 3004. During the process, the call retains its precedence level, 1, which designates Flash Override.
Three-Way Calling

Cisco Unified Communications Manager prescribes the following requirements for three-way calling:

- Each connection of a three-way call must maintain its original precedence level.
- The phone that performs the split operation of the three-way call uses the higher precedence level of the two calls when different precedence levels are involved.

Cisco Unified Communications Manager MLPP also includes preemption of conference bridge resources. If a conference bridge is saturated with calls, individual streams get preempted when setup of a new higher precedence three-way call occurs.

Configuration

Cisco recommends setting the Maximum Ad Hoc Conference service parameter to 3. This setting limits ad hoc calls to three participants. Cisco Unified Communications Manager uses the ad hoc conference feature to implement a three-way call.

Use the Cisco Unified Communications Manager IP Voice Media Streaming App to service three-way calls. Do not use the IOS DSP farm to service conference calls because the IOS DSP farm does not address MLPP support.

Preemption occurs across a single bridge only.

MLPP three-way calls do not interoperate with the conference chaining features that were added in Release 4.2 of Cisco Unified Communications Manager.

Example 1

This example discusses a three-way call among A, B, and C. A called B at Priority 4; then, A called C at Priority 2 (Flash) and started the conference. The conference now proceeds as active with three participants: A at Flash precedence level, B at Priority precedence level, and C at Flash precedence level. When C hangs up, A and B get joined together in a normal call. A must get downgraded from Flash to Priority.

Example 2

In this example, a conference call preempts an existing conference call. The max streams value on the conference bridge was set to 3 to saturate the bridge. The first three-way call gets established among parties A, B, and C at Routine precedence level (5). Phone D then establishes a three-way call with parties E and F at Flash precedence level (2).

Call Transfer

When a switch initiates a call transfer between two segments that have the same precedence level, the segments should maintain the precedence level upon transfer. When a call transfer is made between call segments that are at different precedence levels, the switch that initiates the transfer marks the connection at the higher precedence level of the two segments.

Cisco Unified Communications Manager supports this requirement by upgrading the precedence level of a call leg that is involved in a transfer operation. For example, party A calls party B with Priority precedence level. Party B then initiates a transfer to C and dials the Flash precedence digits when dialing. When the transfer completes, the precedence level of party A gets upgraded from Priority to Flash.
MLPP Supplementary Services

Chapter 35      Multilevel Precedence and Preemption

MLPP Supplementary Services

Note
The precedence level upgrade does not work over a trunk device such as an intercluster trunk (ICT) or PRI trunk.

Configuration
The MLPP transfer service entails no configuration requirements. The feature gets enabled automatically when MLPP is enabled, and the phones support the Transfer softkey.

Call Pickup
Cisco Unified Communications Manager adds the criteria of highest precedence to the call pickup algorithm, including the following requirements:

- If a call pickup group has more than one party in an unanswered condition and the unanswered parties are at different precedence levels, a call pickup attempt in that group retrieves the highest precedence call first.
- If multiple calls of equal precedence are ringing simultaneously, a call pickup attempt in that group retrieves the longest ringing call first.
- The system supports group pickup functionality for MLPP calls. Operation follows normal call pickup functionality.
- For MLPP calls, no support exists for Other Group Pickup.
- If multiple calls are ringing at directory number (DN) A, a user that picks up a call from DN A by using the Directed Call Park feature will be connected to the incoming call of highest precedence, assuming that the user is configured to use the Directed Call Park feature to pick up calls from DN A.

Configuration
The Call Pickup for MLPP capability introduces no special configuration considerations; however, MLPP calls do not support other group pickup.

Hunt Pilots and Hunt Lists
Cisco Unified Communications Manager includes modifications to the previous implementation of the hunt pilot feature. The following aspects of MLPP interaction with hunt pilots changed:

- Normal hunt algorithm logic occurs until all lines in the hunt group are busy.
- When all lines are busy, the lowest precedence call gets selected for preemption.
- When preemption occurs, the normal line group No Answer timer continues. When this timer expires, the next lowest precedence call in the hunt group gets selected for preemption.

MLPP gets implemented for the following hunt algorithms:

- Top down
- Longest idle time
- Circular

Preemption can still occur when the broadcast algorithm is in use. Cisco does not provide explicit support for the broadcast algorithm.
Cisco Unified Communications Manager allows configuration of multiple line groups for a hunt group. The current implementation supports only a single line group under a hunt group. Preemption still occurs when multiple line groups are configured, but the lowest precedence call may not get selected for preemption when more than one line group was configured for a hunt group.

**Configuration**

Hunt pilots and hunt lists require the following configuration:

- Configure only one hunt list in the hunt group. Preemption only happens across the first group in the list.
- Set all hunt group options to *Try next member, but do not go to next group*. This includes the options for No Answer, Busy, and Not Available.
- Set the hunt group algorithm to Top Down, Circular, or Longest Idle Time. Cisco does not provide support for the Broadcast algorithm.
- Disable the *Use personal preferences* check boxes on the hunt pilot.
- Ensure the MLPP precedence setting on the hunt pilot specifies *Default*.
- Configure all stations in the hunt list in a single MLPP domain.

Cisco strongly recommends the following additional configuration:

- Set the Forward No Answer DN hunt pilot to the DN of last resort.
- Set the Forward on Busy DN hunt pilot to the DN of last resort.

**Supplementary Services Support for SCCP Gateway Endpoints**

These updates bring together Supplementary Services support for SCCP gateway endpoints and MLPP support for basic call on SCCP gateways.

---

**Note**

This feature is supported on analog phones only.

The Supplementary Services support update incorporates the following functionalities:

- **Call Hold**—The users can avail of the following functionalities during Call Hold interaction with MLPP on SCCP gateways:
  - Preemption if the new call is higher precedence than both held and active calls.

**Note**

Be aware that Preemption preempts both the held calls, and the active call.

- **Precedence Call Waiting**—The users can avail of the following functionalities during Call Waiting interaction with MLPP on SCCP gateways:
  - Precedence Call Waiting tone support on the gateway
  - For single active call, new higher precedence call preemption rather than play Precedence Call Waiting
  - On a phone with ringing precedence calls, an inbound call preempts the lower precedence ringing calls.
Note

If the user chooses to invoke the Cancel Call Waiting feature while making a call, this overrides the Precedence Call Waiting settings for just that call. The Cancel Call Waiting settings apply only on the phone from which it is invoked, and have no affect on the phones calling it. For more information on the Cancel Call Waiting feature, see the Cisco Unified Communications Manager Administration Guide.

• **Allow Call Waiting During an In-Progress Outbound Analog Call Service Parameter**—A new service parameter is added to Cisco Unified Communications Manager. This parameter determines whether Cisco Unified Communications Manager allows an inbound call to be presented to a call-waiting-enabled SCCP gateway analog phone, when the analog phone is involved in an outbound call but may be unable to play the call waiting tone. The analog phone may not be able to play the call waiting tone until the outbound call gets to the alerting or connected state. Valid values can specify True or False:
  – **True**—The call-waiting-eligible analog phone is presented with the inbound call regardless of the phone's ability to play call waiting tone, and the standard call answer time limit applies.
  – **False**—Cisco Unified Communications Manager treats this as a normal analog line appearance reaching its Busy Trigger call limit; this treatment could involve forwarding actions, tones, or any other features applicable to the trigger.

Note

For information on working with service parameters, see the “Configuring Service Parameters for a Service on a Server” section in Cisco Unified Communications Manager Administration Guide.

**System Requirements for Multilevel Precedence and Preemption**

MLPP requires Cisco Unified Communications Manager 4.0 or later to operate.

**Devices That Support Multilevel Precedence and Preemption**

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support MLPP. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   
   The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application
   
   – by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking **Go**.
   
   – by choosing **File > Cisco Unified Reporting** at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   
   – by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click **System Reports** in the navigation bar.
3. In the list of reports that displays in the left column, click the **Unified CM Phone Feature List** option.

4. Click the **Generate a new report** link to generate a new report, or click the **Unified CM Phone Feature List** link if a report already exists.

5. To generate a report of all IP Phones that support call precedence for MLPP, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   - **Product:** All
   - **Feature:** Call Precedence (for MLPP)

   The List Features pane displays a list of all devices that support the MLPP feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.

6. To generate a report of all IP Phones that support call preemption for MLPP, choose these settings from the respective drop-down list boxes and click the **Submit** button:

   - **Product:** All
   - **Feature:** Call Pre-emption (for MLPP)

   The List Features pane displays a list of all devices that support the MLPP feature. You can click on the Up and Down arrows next to the column headers (**Product** or **Protocol**) to sort the list.


---

**Interactions and Restrictions**

The following sections describe the interactions and restrictions for MLPP.

- Interactions, page 35-39
- Restrictions, page 35-40

**Interactions**

MLPP interacts with the following Cisco Unified Communications Manager features as follows:

- Cisco Extension Mobility—The MLPP service domain remains associated with a user device profile when a user logs in to a device by using extension mobility. The MLPP Indication and Preemption settings also propagate with extension mobility. If either the device or the device profile do not support MLPP, these settings do not propagate.

- Immediate Divert—Immediate Divert diverts calls to voice-messaging mail boxes regardless of the type of call (for example, a precedence call). When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) also gets deactivated.

- Cisco Unified Communications Manager Assistant (Unified CM Assistant)—MLPP interacts with Unified CM Assistant as follows:
  - When Cisco Unified Communications Manager Assistant handles an MLPP precedence call, Cisco Unified Communications Manager Assistant preserves call precedence.
  - Cisco Unified Communications Manager Assistant filters MLPP precedence calls in the same manner as it filters all other calls. The precedence of a call does not affect whether the call is filtered.
Interactions and Restrictions

- Because Cisco Unified Communications Manager Assistant does not register the precedence of a call, it does not provide any additional indication of the precedence of a call on the assistant console.

- Resource Reservation Protocol (RSVP)—RSVP supports MLPP inherently. The “RSVP-Based MLPP” section in the Resource Reservation Protocol chapter of the Cisco Unified Communications Manager System Guide explains how MLPP functions when RSVP is activated.

- Supplementary Services—MLPP interacts with multiple line appearances, call transfer, call forwarding, three-way calling, call pickup, and hunt pilots as documented in the “MLPP Supplementary Services” section on page 35-33 and the subsections that describe the interaction with each service.

Restrictions

The following restrictions apply to MLPP:

- Common Network Facility Preemption support exists only for T1-CAS and T1-PRI (North American) interfaces on targeted Voice over IP gateways that Cisco Unified Communications Manager controls by using MGCP protocol and that have been configured as MLPP Preemption Enabled.

- User Access Channel support exists only for the following Cisco Unified IP Phone models, which must be configured as MLPP Preemption Enabled:
  - Cisco Unified IP Phone 7960, 7962, 7965
  - Cisco Unified IP Phone 7940, 7942, 7945

- IOS gateways support SCCP interface to Cisco Unified Communications Manager. Hence, they support BRI and analog phones which appear on Cisco Unified Communications Manager as supported phone models.

- Only MLPP Indication Enabled devices generate MLPP-related notifications, such as tones and ringers. If a precedence call terminates at a device that is not MLPP Indication Enabled, no precedence ringer gets applied. If a precedence call originates from a device that is not MLPP Indication Enabled, no precedence ringback tone gets applied. If a device that is not MLPP Indication Enabled is involved in a call that is preempted (that is, the other side of the call initiated preemption), no preemption tone gets applied to the device.

- For phones, devices that are MLPP indication disabled (that is, MLPP Indication is set to Off) cannot be preempted. For trunks, MLPP indication and preemption function independently.

- Cisco Unified Communications Manager does not support the Look Ahead for Busy (LFB) option.

- Intercluster trunk MLPP carries precedence information through dialed digits. Domain information does not get preserved and must be configured per trunk for incoming calls.

- 729 Annex A is supported.

- Various location bandwidth preemption limitations exist.

- For the DRSN, CDRs represent precedence levels with values 0, 1, 2, 3, and 4 where 0 specifies Executive Override and 4 specifies Routine, as used in DSN. CDRs thus do not use the DRSN format.
MLPP-enabled devices are not supported in line groups. As such, Cisco recommends the following guidelines:

- MLPP-enabled devices should not be configured in a line group. Route groups, however, are supported. Both trunk selection and hunting methods are supported.
- If an MLPP-enabled device is configured in a line group or route group, in the event of preemption, if the route list does not lock onto the device, the preempted call may be rerouted to other devices in the route/hunt list and preemption indication may be returned only after no devices are able to receive the call.
- Route lists can be configured to support either of two algorithms of trunk selection and hunting for precedence calls. In method 1, perform a preemptive search directly. In method 2, first perform a friendly search. If this search is not successful, perform a preemptive search. Method 2 requires two iterations through devices in a route list.
  
  If route lists are configured for method 2, in certain scenarios involving line groups, route lists may seem to iterate through the devices twice for precedence calls.

Turning on MLPP Indication (at the enterprise parameter, common device configuration, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.

Supplementary Services—MLPP support for supplementary services specifies the following restrictions:

- The current MLPP design addresses only the basic Call Pickup feature and Group Call Pickup feature, not Other Group Pickup. Support for the Directed Call Pickup feature functions as described in the “Call Pickup” section on page 35-36.
- Call Forward All (CFA) support for inbound MLPP calls always forwards the call to the MLPP Alternate Party (MAP) target of the called party, if the MAP target has been configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call gets rejected, and the calling party receives reorder tone.
- Call Forward No Answer (CFNA) support for inbound MLPP calls forwards the call once to a CFNA target. After the first hop, if the call remains unanswered, the call gets sent to the MAP target of the original called party, if the MAP target has been configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call gets rejected, and the calling party receives reorder tone.
- Call Forward Busy (CFB) support for inbound MLPP calls forwards the call up to the maximum number that has been configured for forwarding hops. If the maximum hop count gets reached, the call gets sent to the MAP target of the original called party, if the MAP target has been configured. In the event of an incorrect configuration (that is, no MAP target is specified), the call gets rejected, and the calling party receives reorder tone.
- For hunt pilot support, the hunt group algorithm must specify Longest Idle Time, Top Down, or Circular. Ensure the hunt group options for busy treatment, no answer treatment, and unregistered treatment are set to *Try next member, but do not go to next group*. Preemption only occurs across a single hunt group.

See the “Configuration Checklist for MLPP” section on page 35-1 for configuration details.

**Installing and Activating MLPP**

MLPP, a system feature, comes standard with Cisco Unified Communications Manager software and does not require special installation.
Configuring MLPP

This section contains information on the following topic:

- Setting the Enterprise Parameters for MLPP, page 35-42

Tip

Before you configure MLPP, review the “Configuration Checklist for MLPP” section on page 35-1.

Setting the Enterprise Parameters for MLPP

Cisco Unified Communications Manager provides the following enterprise parameters that apply to MLPP. Set the MLPP-related enterprise parameters as indicated to allow MLPP service.

- **MLPP Domain Identifier**—Default specifies zero (0). Set this parameter to define a domain. Because MLPP service applies to a domain, Cisco Unified Communications Manager only marks connections and resources that belong to calls from MLPP users in a given domain with a precedence level. Cisco Unified Communications Manager can preempt only lower precedence calls from MLPP users in the same domain.

  **Note**  
  You must reset all devices for a change to this parameter to take effect.

- **MLPP Indication Status**—Default specifies **MLPP Indication turned off**. This parameter specifies whether devices use MLPP tones and special displays to indicate MLPP precedence calls. To enable MLPP indication across the enterprise, set this parameter to **MLPP Indication turned on**.

  **Note**  
  You must reset all devices for a change to this parameter to take effect.

- **MLPP Preemption Setting**—Default specifies **No preemption allowed**. This parameter determines whether devices should apply preemption and preemption signaling (such as preemption tones) to accommodate higher precedence calls. To enable MLPP preemption across the enterprise, set this parameter to **Forceful Preemption**.

  **Note**  
  You must reset all devices for a change to this parameter to take effect.

- **Precedence Alternate Party Timeout**—Default specifies 30 seconds. In a precedence call, if the called party subscribes to alternate party diversion, this timer indicates the seconds after which Cisco Unified Communications Manager will divert the call to the alternate party if the called party does not acknowledge preemption or does not answer a precedence call.

- **Use Standard VM Handling For Precedence Calls**—Default specifies **False**. This parameter determines whether a precedence call will forward to the voice-messaging system. If the parameter is set to False, precedence calls do not forward to the voice-messaging system. If the parameter is set to True, precedence calls forward to the voice-messaging system. For MLPP, the recommended setting for this parameter is False, as users, not the voice-messaging system, should always answer precedence calls.

For more information about enterprise parameters, see the **Enterprise Parameter Configuration** chapter of the *Cisco Unified Communications Manager Administration Guide*. 


Additional Information

See the “Related Topics” section on page 35-43.

Related Topics

- Configuration Checklist for MLPP, page 35-1
- Introducing MLPP, page 35-3
- MLPP Supplementary Services, page 35-33
- Interactions and Restrictions, page 35-39
- Installing and Activating MLPP, page 35-41
- Configuration Checklist for MLPP, page 35-1
- Setting the Enterprise Parameters for MLPP, page 35-42
- MLPP Domain Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Resource Priority Namespace Network Domain Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Resource Priority Namespace List Configuration Settings, Cisco Unified Communications Manager Administration Guide
- Call Admission Control, Cisco Unified Communications Manager System Guide
- Resource Reservation Protocol, Cisco Unified Communications Manager System Guide
- Common Device Configuration, Cisco Unified Communications Manager Administration Guide
- Enterprise Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Automated Alternate Routing Group Configuration, Cisco Unified Communications Manager Administration Guide
- Partition Configuration, Cisco Unified Communications Manager Administration Guide
- Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide
- Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Translation Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Annunciator, Cisco Unified Communications Manager System Guide
- Annunciator Configuration, Cisco Unified Communications Manager Administration Guide
- Gateway Configuration, Cisco Unified Communications Manager Administration Guide
- Trunk Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Default Device Profile Configuration, Cisco Unified Communications Manager Administration Guide
- Annunciator Configuration, Cisco Unified Communications Manager Administration Guide
- Route Pattern Configuration, Cisco Unified Communications Manager Administration Guide
Related Topics

- Translation Pattern Configuration, Cisco Unified Communications Manager Administration Guide
- Locations, Cisco Unified Communications Manager System Guide

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager, Cisco Unified IP Phone Models 7960G and 7940G
CHAPTER 36

Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.

This chapter covers the following topics:

- Configuration Checklist for Music On Hold, page 36-1
- Configuration Checklist for Multicast, page 36-3
- Configuration Checklist for Monitoring Music On Hold Performance, page 36-4
- Introducing Music On Hold, page 36-4
- Music On Hold Server, page 36-11
- Music On Hold Audio Sources, page 36-12
- Music On Hold System Requirements and Limits, page 36-16
- Music On Hold Failover and Fallback, page 36-18
- Music On Hold Audio Source Configuration, page 36-18
- Fixed Music On Hold Audio Source Configuration, page 36-23
- Music On Hold Server Configuration, page 36-25
- Music On Hold Audio File Management Configuration, page 36-33
- Related Topics, page 36-36

Configuration Checklist for Music On Hold

The integrated Music On Hold (MOH) feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.
Table 36-1 provides a checklist for configuring music on hold. For more information on music on hold, see the “Introducing Music On Hold” section on page 36-4 and the “Related Topics” section on page 36-36.

### Table 36-1 Music On Hold Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>The Cisco IP Voice Media Streaming application gets installed automatically upon installation of Cisco Unified Communications Manager. To provide an MOH server, you must use the Cisco Unified Serviceability application to activate the Cisco IP Voice Media Streaming application. When a server gets added, the Cisco Unified Communications Manager automatically adds the media termination point, conference bridge, annunciator, and music on hold devices to the database. <strong>Note</strong> During installation, Cisco Unified Communications Manager installs and configures a default music on hold audio source if one does not exist. Music on hold functionality can proceed by using this default audio source without any other changes.</td>
<td>Installing Cisco Unified Communications Manager Release 8.5(1)</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Run the music on hold audio translator.</td>
<td>Music On Hold Audio Sources, page 36-12</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td></td>
</tr>
<tr>
<td>If the audio translator translates files on the same server as the Cisco Unified Communications Manager, serious problems may occur. The audio translator tries to use all available CPU time, and Cisco Unified Communications Manager may experience errors or slowdowns.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>The installation program performs the following actions automatically. If the user manually adds the music on hold components, ensure the following steps are performed.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Configure the music on hold server.</td>
<td>Configuring a Music On Hold Server, page 36-27</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Add and configure audio source files.</td>
<td>Finding a Music On Hold Audio Source, page 36-19</td>
</tr>
</tbody>
</table>
# Configuration Checklist for Multicast

Table 36-2 provides a checklist for configuring various Cisco Unified Communications Manager services to allow multicasting. You must perform all steps for multicast to be available.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure a music on hold server to enable multicast audio sources.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>Cisco strongly recommends incrementing multicast on IP address in firewall situations. This results in each multicast audio source having a unique IP address and helps to avoid network saturation.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure an audio source to allow multicasting.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Create a media resource group and configure it to use multicast for MOH audio.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Create a media resource group list with a multicast media resource group as the primary media resource group.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Choose the media resource group list that was created in Step 4 for either a device pool or for specific devices.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>If necessary, configure the service parameters that affect multicast MOH.</td>
</tr>
</tbody>
</table>
Configuration Checklist for Monitoring Music On Hold Performance

Perform the activities in Table 36-3 to monitor music on hold performance.

Table 36-3  Music On Hold Performance Monitoring

<table>
<thead>
<tr>
<th>Monitoring Activity</th>
<th>Detailed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Use the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT) to check resource usage and device recovery state.</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Real Time Monitoring Tool Administration Guide</em>&lt;br&gt;<em>Cisco Unified Serviceability Administration Guide</em> documents another method of viewing this information.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Search the event log for Cisco IP Voice Media Streaming application entries.</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Serviceability Administration Guide</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Verify that the Cisco IP Voice Media Streaming application service is running.</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Serviceability Administration Guide</em> documents another method of viewing this information.&lt;br&gt;<em>Related Topics, page 36-36</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Search the Media Application trace (CMS) to see what music on hold-related activity that it detects.</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified Serviceability Administration Guide</em></td>
</tr>
</tbody>
</table>

**Additional Information**

See the “Related Topics” section on page 36-36.

Introducing Music On Hold

The following sections explain the Music On Hold feature by providing definitions, service characteristics, feature functionality with examples, and supported features.

**Additional Information**

See the “Related Topics” section on page 36-36.

Music On Hold Definitions

In the simplest instance, music on hold takes effect when phone A is talking to phone B, and phone A places phone B on hold. If Music On Hold (MOH) resource is available, phone B receives music that is streamed from a music on hold server.

The following definitions provide important information for the discussion that follows:

- MOH server—A software application that provides music on hold audio sources and connects a music on hold audio source to a number of streams.
- Media resource group—A logical grouping of media servers. You may associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control server usage or desired service type (unicast or multicast).
• Media resource group list—A list that comprises prioritized media resource groups. An application can select required media resources from among ones that are available according to the priority order that is defined in a media resource group list.

• Audio source ID—An ID that represents an audio source in the music on hold server. The audio source can compose either a file on a disk or a fixed device from which a source stream music on hold server obtains the streaming data. A MOH server can support up to 51 audio source IDs (1 to 51). Each audio source (represented by an audio source ID) can stream as unicast and multicast mode, if needed.

• Holding party—In an active, two-party call, the party that initiates a hold action (either user hold or network hold). Example: If party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party A represents the holding party.

• Held party—In an active, two-party call, the party that does not initiate a hold action but is involved. Example: If party A is talking to party B, and party A presses the Hold softkey to initiate a hold action, party B represents the held party.

The following audio source ID selection rules apply for selecting audio source IDs and media resource group lists:

• The system administrator, not the end user, defines (configures) audio source IDs.
• The system administrator chooses (configures) audio source IDs for device(s) or device pool(s).
• Holding parties define which audio source ID applies to held parties.
• Cisco Unified Communications Manager implements four levels of prioritized audio source ID selection with level four as highest priority and level one as lowest priority.
  - The system selects audio source IDs at level four, which is directory/line-based, if defined. (Devices with no line definition, such as gateways, do not have this level.)
  - If no audio source ID is defined in level four, the system searches any selected audio source IDs in level three, which is device based.
  - If no level four nor level three audio source IDs are selected, the system selects audio source IDs that are defined in level two, which is Common Device Configuration-based.
  - If all higher levels have no audio source IDs selected, the system searches level one for audio source IDs, which are clusterwide parameters.

The following media resource group list selection rules apply:

• Held parties determine the media resource group list that a Cisco Unified Communications Manager uses to allocate a music on hold resource.

• Two levels of prioritized media resource group list selection exist:
  - Level two media resource group list provides the higher priority level, which is device based. Cisco Unified Communications Manager uses the media resource group list at the device level if such a media resource group list is defined.
  - Level one media resource group list provides the lower priority level, which is an optional DevicePool parameter. Cisco Unified Communications Manager uses the DevicePool level media resource group list only if no media resource group list is defined in the device level for that device.

• If no media resource group lists are defined, Cisco Unified Communications Manager uses the system default resources. System default resources comprise resources that are not assigned to any existing media resource group. Be aware that system default resources are always unicast.
Music On Hold Characteristics

The integrated Music On Hold feature allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. This source makes music available to any possible on-net or off-net device that is placed on hold. On-net devices include station devices and applications that are placed on hold, consult hold, or park hold by an interactive voice response (IVR) or call distributor. Off-net users include those who are connected through Media Gateway Control Protocol (MGCP)/skinny gateways, IOS H.323 gateways, and IOS Media Gateway Control Protocol gateways. The system also makes the Music On Hold feature available for Cisco IP POTS phones that connect to the Cisco IP network through FXS ports on IOS H.323/Media Gateway Control Protocol and for Cisco Media Gateway Control Protocol/skinny gateways.

The integrated Music On Hold feature covers media server, data base administration, call control, media resource manager, and media control functional areas.

The music on hold server provides the music resources/streams. These resources register with the Cisco Unified Communications Manager during the initialization/recovery period.

Database administration provides a user interface to allow the Cisco Unified Communications Manager administrator to configure the Music On Hold feature for the device(s). Database administration also provides Cisco Unified Communications Manager call control with configuration information.

Call control controls the music on hold scenario logic.

The media resource manager processes the registration request from the music on hold server and allocates/deallocates the music on hold resources under the request of call control.

Media control controls the establishment of media stream connections, which can be one-way or two-way connections.

You must ensure that an end device is provisioned with information that is related to music on hold before music on hold functions for that device. Initializing a Cisco Unified Communications Manager creates a media resource manager. The music on hold server(s) registers to the media resource manager with its music on hold resources.

When an end device or feature places a call on hold, Cisco Unified Communications Manager connects the held device to a music resource. When the held device is retrieved, it disconnects from the music on hold resource and resumes normal activity.

Additional Information

See the “Related Topics” section on page 36-36.
Music On Hold Functionality

For music on hold to function, you must perform the actions in the following list:

- Configure music on hold servers.
- Configure audio sources. For the examples that follow, configure and provision the following audio sources: Thank you for holding and Pop Music 1.

**Note** Define audio sources first and then set up the music on hold servers, especially when multicast will be used. The user interface allows either step to take place first.

**Note** If an audio source is configured for multicast, the MOH server always transmits the audio stream, regardless of whether devices are held.

- Configure media resource groups. If multicast is desired, check the Use Multicast for MOH Audio check box.

**Note** CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

- Configure media resource group lists.
- Assign media resource group lists and audio sources to device pools.
- Assign media resource group lists and audio sources to devices (to override assignments made to device pools).
- Assign audio sources to lines (to override device settings).

Using the preceding configuration actions, if you define music on hold functionality as follows, the examples that follow demonstrate music on hold functionality for user hold, transfer hold, and call park.

**Media Resource Groups**

MOH designates a music on hold server. MRG designates a media resource group.

- MRG_D comprises MOH_D.
- MRG_S_D comprises MOH_S and MOH_D.

**Media Resource Group Lists**

MRGL designates a media resource group list.

- MRGL_D comprises MRG_D.
- MRGL_S_D comprises MRG_S_D and MRG_D (prioritized order).

**Nodes**

- Dallas node comprises phone D and MOH_D.
- San Jose node comprises phone S and MOH_S.
Assign phone D audio source ID 5, Thank you for holding or plain music (for both user and network hold), and MRGL_D.

Assign phone S audio source ID 1, Pop Music 1 (for both user and network hold), and MRGL_S_D.

User Hold Example

Phone D calls phone S, and phone S answers. Phone D presses the Hold softkey. Result: Phone S receives Thank you for holding announcement or plain music that is streaming from MOH_S. (MOH_S has available streams.) When phone D presses the Resume softkey, phone S disconnects from the music stream and reconnects to phone D.

Transfer Hold Example

Transfer hold serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone D presses the Transfer softkey. Phone S receives Thank you for holding announcement or plain music that is streaming from MOH_D. (MOH_S has no available streams, but MOH_D does.) After phone D completes the transfer action, phone S disconnects from the music stream and gets redirected to phone X, the transfer destination.

Call Park Example

Call park serves as an example of network hold.

Phone D calls phone S, and phone S answers. Phone S presses the CallPark softkey. Phone D receives a beep tone. (MOH_D has no available streams.) Phone X picks up the parked call. Phone S gets redirected to phone X (phone D and phone X are conversing).

Additional Information

See the “Related Topics” section on page 36-36.

Supported Music On Hold Features

Music on hold supports the following features, which are listed by category. Feature categories include music on hold server characteristics, server scalability, server manageability, server redundancy, database scalability, and manageability.

Music On Hold Server Characteristics

- Servers stream music on hold from music on hold data source files that are stored on their disks.
- Servers stream music on hold from an external audio source (for example, looping tape recorder, radio, or CD).
- Music on hold servers can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the local server of each music on hold server always stores the music on hold data source files. Cisco Unified Communications Manager does not support distribution of fixed-device (hardware) audio sources across music on hold servers within a media resource group.
- Music on hold data source files have a common filename across all music on hold servers.
- You must ensure that music on hold data source files are uploaded to each MOH server.
Introducing Music On Hold

Each audio source receives a feed from either a designated file or a designated fixed source (for example, radio or CD).

A designated fixed source comprises a single device, which is either enabled or disabled.

The audio driver on the local machine makes a single fixed source available to the music on hold server.

Music on hold servers support the G.711 (a-law and mu-law), G.729a, and wideband codecs.

Music on hold servers register with one primary Cisco Unified Communications Manager server.

Server Scalability

Music on hold supports from 1 to 500 simplex unicast streams per music on hold server.

Music on hold supports multiple Cisco-developed media-processing applications, including Interactive Voice Response (IVR) and Auto-Attendant (AA). Cisco Unified Communications Manager facilitates this support.

Music on hold server simultaneously supports up to 50 music on hold data source files as sources.

Music on hold server supports one fixed-device stream source in addition to the file stream sources. This source comprises the fixed audio source, which gets configured on the Fixed MOH Audio Source Configuration window. This source requires the additional Cisco USB Music-On-Hold-capable adapter.

Server Manageability

From Cisco Unified Serviceability windows, you can activate the music on hold server application, Cisco IP Media Streaming Application, on any standard media convergence server (MCS) as a service.

You can activate music on hold application on the same media convergence server (MCS) as other media applications, so music on hold and the other media application(s) co-reside on the MCS.

You can install music on hold server application on multiple media convergence servers (MCS) in a cluster.

A Cisco Unified Communications Manager cluster supports a mix of Cisco Media Convergence Server (MCS) and Cisco Unified Computing System (UCS) nodes. If you want to use the Music On Hold feature with an external source (USB audio dongle), you must use an MCS server for the node(s) that supply MOH from an external source.

The administrator can specify the source for each source stream that the server provides.

Administration of stream sources takes place through a browser.

Server Redundancy

Music on hold servers support Cisco Unified Communications Manager lists. The first entry on the list serves as the primary server, and subsequent Cisco Unified Communications Managers on the list serve as backup Cisco Unified Communications Managers in prioritized order.

Music on hold servers can maintain a primary and backup connection to Cisco Unified Communications Managers from their Cisco Unified Communications Manager list.

Music on hold servers can re-home to backup Cisco Unified Communications Managers by following the standard procedures that are used by other servers and phones on the cluster.

Music on hold servers can re-home to their primary server by following standard procedures for other media servers on the cluster.
Introducing Music On Hold

When a Cisco Unified Communications Manager is handling a call and places either endpoint in the call on hold, the Cisco Unified Communications Manager can connect the held endpoint to music on hold. This feature applies for both network hold and user hold. Network hold includes transfer, conference, call park, and so forth.

A media resource group for music on hold supports having a single music source stream for all connected streams.

The system supports having music on hold server(s) at a central site without music on hold server(s) at remote sites. Remote site devices that require music on hold service can obtain service from a media resource group across the WAN when service is not available locally.

You can distribute music on hold servers to any site within a cluster.

A music on hold server can use a single music on hold data source for all source streams and, hence, all connected streams. When multiple music on hold servers are involved, the music on hold data source may comprise a file that is stored locally on each server.

The system can detect when the primary media resource group that supplies music on hold for a device is out of streams and can select a stream from the secondary or tertiary media resource group that is specified for that device.

When it connects a device to music on hold, the system can insert a transcoder when needed to support low-bandwidth codecs.

Database Scalability

Cisco Unified Communications Manager can support from 1 to 500 unicast sessions per music on hold server.

A cluster can support from 1 to more than 20 music on hold servers.

A cluster can support from 1 to more than 10,000 simultaneous music on hold streams across the cluster.

A cluster can support from 1 to 500 or more media resource groups for music on hold.

A media resource group for music on hold can support from 1 to 20 or more music on hold servers.

Manageability

The administrator can select media resource group list per device.

The administrator can select music on hold source stream per device/DN.

The administrator can select music on consult (network hold) source stream per device/DN.

The administrator can configure which music on hold servers are part of a specified media resource group.

The administrator can designate primary, secondary, and tertiary music on hold/consult servers for each device by configuring media resource groups and media resource group lists.

The administrator can provision multiple music on hold servers.

The administrator can provision any device that is registered with the system such that any music on hold server can service it in the system.

All music on hold configuration and administration take place through a browser.

The administrator specifies the user hold and network hold audio sources for each device pool. These default audio sources may function as either file based or fixed device based.
The administrator can designate a music on hold server as either unicast or multicast, provided that resources exist to support multicast.

**Note**
CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

The administrator can reset all music on hold servers.

**Additional Information**
See the “Related Topics” section on page 36-36.

---

**Music On Hold Server**

The music on hold server uses the Station Stimulus (Skinny Client) messaging protocol for communication with Cisco Unified Communications Manager. A music on hold server registers with the Cisco Unified Communications Manager as a single device and reports the number of simplex, unicast audio streams that it can support. The music on hold server advertises its media type capabilities to the Cisco Unified Communications Manager as G.711 mu-law and a-law, G.729a, and wideband. Cisco Unified Communications Manager starts and stops music on hold unicast streams by sending skinny client messages to the music on hold server.

A music on hold server handles up to 500 simplex, unicast audio streams. A media resource group includes one or more music on hold servers. A music on hold server supports 51 audio sources, with one audio source that is sourced from a fixed device that uses the local computer audio driver, and the rest that are sourced from files on the local music on hold server.

You may use a single file for multiple music on hold servers, but the fixed device may be used as a source for only one music on hold server. The music on hold audio source files get stored in the proper format for streaming. Cisco Unified Communications Manager allocates the simplex unicast streams among the music on hold servers within a cluster.

The music on hold server uses the media convergence server series hardware platform. A Cisco USB sound adapter that is installed on the same computer as the music on hold server application provides the external fixed audio source, which can be a looping tape recorder, radio, or CD.

The music on hold server, which is actually a component of the Cisco IP Voice Media Streaming application, supports standard device recovery and database change notification.

Each music on hold server uses the local hard disk to store copies of the Music On Hold audio source files. Each audio source file gets distributed to the server(s) when the file is added through the Cisco Unified Communications Manager Administration interface.

**Note**
The administrator must upload Music On Hold audio source files to each MOH server.

**Additional Information**
See the “Related Topics” section on page 36-36.
Music On Hold Audio Sources

When the administrator imports an audio source file, the Cisco Unified Communications Manager Administration window interface processes the file and converts the file to the proper format(s) for use by the music on hold server.

- The recommended format for audio source files includes the following specifications:
  - 16-bit PCM wav file
  - Stereo or mono
  - Sample rates of 48 kHz, 32 kHz, 16 kHz, or 8 kHz

**Additional Information**
See the “Related Topics” section on page 36-36.

Creating Audio Sources

Most standard wav files serve as valid input audio source files, including the following file types:

- 16-bit PCM (stereo/mono)
- 8-bit CCITT a-law or mu-law (stereo/mono)

**Note**
The Music On Hold feature does not support the MP3 format.

In creating an audio source, the following sequence takes place:

- The administrator imports the audio source file into the Cisco Unified Communications Manager music on hold server. This step may take some time to transfer the file and convert the file to the proper format(s) for the music on hold server to use.
- The administrator must import the audio source file to each MOH server in each cluster prior to assigning an audio source number to the audio source file.
- The music on hold server uses the local audio source file(s).
- The music on hold server streams the files by using a kernel mode RTP driver as Cisco Unified Communications Manager needs or requests.

**Additional Information**
See the “Related Topics” section on page 36-36.

Storing Audio Source Files

In previous releases, Cisco Unified Communications Manager did not limit the amount of space that MOH files used. The MOH upload tool does not limit the number of uploaded files or the file size. The modified upload JSP pages check the disk usage of existing MOH files and only permit uploads if sufficient space is found.

**Note**
The smallest node on the cluster controls MOH capacity.
Managing Audio Sources

After music on hold audio sources are created, their management occurs entirely through Cisco Unified Communications Manager Administration. Choose Media Resources > Music On Hold Audio Source to display the Music On Hold (MOH) Audio Source Configuration window. For a given audio source, use this window to add, update, or delete a music on hold audio source. For each audio source file, assign a music on hold audio source number and music on hold audio source name and decide whether this audio source will play continuously and allow multicasting. For an audio source, this window also displays the music on hold audio source file status. See the “Finding a Music On Hold Audio Source” section on page 36-19 for details.

Additional Information
See the “Related Topics” section on page 36-36.

Multicast and Unicast Audio Sources

Multicast music on hold conserves system resources. Multicast allows multiple users to use the same audio source stream to provide music on hold. Multicast audio sources associate with an IP address. Unicast music on hold, the system default, uses a separate source stream for each user or connection. Users connect to a specific device or stream.

The MOH feature causes any party that gets placed on hold to hear the same point of the audio source that is streaming, regardless of when the party is placed on hold.

If you are using the MOH to deliver a spoken announcement when a party is placed on hold, the standard MOH configuration can create a problem. Users do not hear the announcement from the beginning, except for the first party that gets placed on hold: other parties join the announcement (audio source) in progress.

Both multicast and unicast configurations present the same audio-source behavior to held parties. Each audio source gets used once, and the stream gets split internally and gets sent to the held parties. The only difference between multicast and unicast, in this case, is how the data itself gets sent over the network.

Thus, basic MOH configuration is unsuitable for playing announcements that users must hear from the beginning.

For administrators, multicast entails managing devices, IP addresses, and ports. In contrast, unicast entails managing devices only.
For multicast, administrators must define at least one audio source to allow multicasting. To define music on hold servers for multicast, first define the server to allow multicasting.

For multicast, an address comprises a combination of an IP address and a port number. Each audio source for multicast requires a set of addresses: one for each format on each MOH server. When configuring the MOH server for multicast, specify whether addresses should be assigned by incrementing the port or the IP address.

Cisco strongly recommends incrementing multicast on IP address instead of port number to avoid network saturation in firewall situations. If you follow this recommendation, each multicast audio source has a unique IP address, and you help to avoid network saturation.

The Max Hops field in the Music On Hold (MOH) Server Configuration window indicates the maximum number of routers that an audio source is allowed to cross. If max hops is set to zero, the audio source must remain in its own subnet. If max hops is set to one, the audio source can cross up to one router to the next subnet. Cisco recommends setting max hops to two.

A standards body reserves IP addresses. Addresses for IP multicast range from 224.0.1.0 to 239.255.255.255. The standards body, however, assigns addresses in the range 224.0.1.0 to 238.255.255.255 for public multicast applications. Cisco strongly discourages using public multicast addresses for music on hold multicast. Instead, Cisco recommends using an IP address in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 to 239.255.255.255).

Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

Multicast functions only if both media resource groups and media resource group lists are defined to include a multicast music on hold server. For media resource groups, you must include a music on hold server that is set up for multicast. Such servers get labeled as (MOH)[Multicast]. Also, check the Use Multicast for MOH Audio check box when you define a media resource group for multicast.

For media resource group lists, which are associated with device pools and devices, define the media resource group list, so the media resource group that is set up for multicast is the first group in the list. This recommended practice facilitates the device efforts to find the multicast audio source first.

In music on hold processing, the held device (the device placed on hold) determines the media resource to use, but the holding device (the device that initiates the hold action) determines the audio source to use.

The following restriction exists for multicast music on hold (MOH) when a media termination point (MTP) is invoked. When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, the caller receives silence instead of music on hold. To avoid this scenario, configure unicast MOH or Tone on Hold instead of multicast MOH.

CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.
**Multicast MOH Direction Attribute for SIP Service Parameter**

The Multicast MOH Direction Attribute for SIP service parameter determines whether Cisco Unified Communications Manager sets the direction attribute of the Session Description Protocol (SDP) in its multicast Music on Hold (MOH) INVITE message to sendOnly or recvOnly.

If your deployment uses SIP phone loads 8.4 and earlier for Cisco Unified IP Phones 7940 and 7960, or SIP phone loads 8.1(x) and earlier for Cisco Unified IP Phones 7906, 7911, 7941, 7961, 7970, and 7971, set this parameter to sendOnly. Otherwise, leave this parameter set to the default value, recvOnly.

**Multicast Music On Hold Over H.323 Intercluster Trunks**

The Multicast Music on Hold (MOH) Over H.323 Intercluster Trunk feature allows multicast MOH to work over H.323 intercluster trunks (ICTs). Prior to the implementation of this feature, multicast MOH used bandwidth for each unicast MOH over the same ICT, which wasted bandwidth.

Prior to the implementation of this feature, the H.323 Open Logical Channel (OLC) ACK message carried the IP address and port for multicast MOH. With the implementation of this feature, the H.323 OLC message now carries the IP address and port for multicast MOH, and Cisco Unified Communications Manager adds the mechanism to handle the information in the H.323 OLC message.

When a call connects over an intercluster trunk and one of the parties presses the Hold key, MOH streams over the intercluster trunk. If multicast MOH is turned on and the holding party and trunk are configured to use the multicast MOH server, MOH streams with multicast. Only one multicast MOH stream streams over the trunk regardless how many calls are put on hold on this trunk.

**Send Multicast MOH in H.245 OLC Message Service Parameter**

The service parameter, Send Multicast MOH in H.245 OLC Message, controls the Multicast Music On Hold Over H.323 Intercluster Trunk feature. Both Cisco Unified Communications Manager nodes that are involved in a call must support single-transmitter multicast for the setting of this parameter to have any effect. This service parameter affects only the side of the party that places the call on hold and does not affect how the far end carries the multicast transport address. Even if this parameter is turned off, multicast MOH applies for the held-party side of the call as long as the held party has the capability to support single-transmitter multicast.

If you want to configure this feature via the clusterwide service parameter, Send Multicast MOH in H.245 OLC Message, which supports the Cisco CallManager service, choose System > Service Parameters in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Send Multicast MOH in H.245 OLC Message drop-down list box, choose True.

The service parameter governs the multicast MOH behavior on H.323 intercluster trunks and devices. The new service parameter does not control multicast MOH over SIP trunks because multicast MOH over SIP trunks does not constitute a new behavior.

**Cisco Unified Communications Manager Administration Configuration Tips**

Calls that connect over Cisco Unified Communications Manager intercluster trunks use this feature for multicast MOH. This feature does not work if any middle box between Cisco Unified Communications Managers does not pass the new fields in Terminal Capability Set (TCS) and OLC message.

No additional configuration exists for this new feature in addition to the normal configuration for setting up multicast MOH. This feature only applies between Cisco Unified Communications Managers that support single-transmitter multicast.
Music On Hold System Requirements and Limits

The feature remains active by default. To turn off the feature, set the value of the Send Multicast MOH in H.245 OLC Message service parameter to **False**. Do so to resolve interoperability issues that the feature may cause.

**Note**
Multicast MOH does not support interoperability between H.323 and SIP protocols.

**Additional Information**
See the “Related Topics” section on page 36-36.

Music On Hold System Requirements and Limits

The following system requirements and limits apply to the Music On Hold feature:

- All audio streaming devices that are using the Music On Hold feature support simplex streams. The music on hold server supports up to 500 simplex streams.

- The music on hold (MOH) server, a part of the Cisco IP Voice Media Streaming application, gets installed with Cisco Unified Communications Manager. Use the Cisco Unified Serviceability application to activate the MOH server. Because only one Cisco IP Voice Media Streaming application may be activated on a media convergence server, you can enable only one MOH server per server. You can activate the Cisco IP Voice Media Streaming application, however, on multiple servers to provide multiple MOH servers for the cluster.

- For a Cisco Unified Communications Manager cluster, you may define up to 50 audio sources. A Cisco Unified Communications Manager Administration window supports import, addition, update, and deletion of each audio source. The music on hold server also supports one fixed input source. The system supports the following codecs: G.711 a-law/mu-law, G.729a, and wideband.

**Note**
Because the G.729a codec is designed for human speech, using it with music on hold for music may not provide acceptable audio quality.

- For each cluster, you may define up to 50 audio sources from files as well as one fixed audio source. A Cisco Unified Communications Manager Administration window supports addition, update, and deletion of each audio source. All servers use local copies of the same 50 or fewer files. You must set up the fixed audio source that is configured on each MOH server.

- For each cluster, you may define at most 20 music on hold servers. The Cisco Unified Communications Manager Administration window allows update of music on hold servers. The MOH server automatically gets added when a server gets added. You cannot delete the MOH server unless the server gets deleted. The window allows administrators to specify the following characteristics for each MOH server:
  - Name
  - Node (server host name)
  - Device pool
  - Maximum number of unicast and multicast streams
  - Sources to multicast
  - For each multicast source: IP address, port, and time to live (maximum number of router hops)
Cisco Unified Communications Manager Administration allows definition of at least 500 media resource groups per cluster. Each media resource group may include any combination of at least 20 media resources, including music on hold servers, media termination points, transcoders, and conference devices. Music on hold servers in one cluster support at least 10,000 simultaneous music on hold streams. See “Media Resource Groups” in the Cisco Unified Communications Manager System Guide for details of media resource groups.

Cisco Unified Communications Manager Administration allows definition of media resource group lists. See “Media Resource Group Lists” in the Cisco Unified Communications Manager System Guide for details of media resource group lists.

Modifications to the Cisco Unified Communications Manager Administration device configuration windows for phones and gateways allow the selection of a media resource group list, hold stream source, and consult stream source as optional parameters for a device.

Modifications to the Cisco Unified Communications Manager Administration Directory Number configuration windows allow selection of a user hold source and a network hold source.

Modifications to the Cisco Unified Communications Manager Administration Service Parameters allows entry to a clusterwide, default music on hold stream source (default specifies 1) and default media resource group type (default specifies unicast).

The number of streams that the music on hold server can use may decrease if the annunciator, software MTP, or software conference bridge is in use on the same MCS server.

The following restriction exists for multicast music on hold (MOH) when a media termination point (MTP) is invoked. When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, the caller receives silence instead of music on hold. To avoid this scenario, configure unicast MOH or Tone on Hold instead of multicast MOH.

CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

Multicast MOH does not support interoperability between H.323 and SIP protocols.

The IP Voice Media Streaming Application, which is a component of Music On Hold, supports IPv4. Cisco Unified Communications Manager does not support IPv6 with multicast music on hold, so devices with an IP Addressing Mode of IPv6 Only cannot support multicast music on hold. Under these circumstances, Cisco Unified Communications Manager plays a tone, instead of music, when the phone is on hold. For phones that have an IP Addressing Mode of IPv6 Only and that use unicast music on hold, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa) into the media stream. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

The Fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Cisco Unified Communications Manager does not support USB when running on VMware. VMware does, however, support internal Music On Hold.

A Cisco Unified Communications Manager cluster supports a mix of Cisco Media Convergence Server (MCS) and Cisco Unified Computing System (UCS) nodes. If you want to use the Music On Hold feature with an external source (USB audio dongle), you must use an MCS server for the node(s) that supply MOH from an external source.

**Additional Information**

See the “Related Topics” section on page 36-36.
Music On Hold Failover and Fallback

The music on hold server supports Cisco Unified Communications Manager lists and failover as implemented by the software conference bridge and media termination point. Upon failover, the system maintains connections to a backup Cisco Unified Communications Manager if one is available.

Cisco Unified Communications Manager takes no special action when a music on hold server fails during an active music on hold session. The held party receives nothing from this point, but this situation does not affect normal call functions.

Additional Information
See the “Related Topics” section on page 36-36.

Configuring Music On Hold

This section contains information on the following topics:

- Music On Hold Audio Source Configuration, page 36-18
- Fixed Music On Hold Audio Source Configuration, page 36-23
- Music On Hold Server Configuration, page 36-25
- Music On Hold Audio File Management Configuration, page 36-33
- Viewing Music On Hold Server Performance, page 36-36
- Checking Service States, page 36-36

Tip
Before you configure music on hold, review the “Configuration Checklist for Music On Hold” section on page 36-1, the “Configuration Checklist for Multicast” section on page 36-3, and the “Configuration Checklist for Monitoring Music On Hold Performance” section on page 36-4.

Music On Hold Audio Source Configuration

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music streamed from a streaming source. This feature includes the following actions:

- End user hold
- Network hold, which includes transfer hold, conference hold, and park hold


Use the following topics to configure Music On Hold audio sources:

- Finding a Music On Hold Audio Source, page 36-19
- Configuring a Music On Hold Audio Source, page 36-20
- Deleting a Music On Hold Audio Source, page 36-21
- Music On Hold Audio Source Configuration Settings, page 36-21
Finding a Music On Hold Audio Source

Because you might have multiple Music On Hold audio sources in your network, Cisco Unified Communications Manager lets you search for Music On Hold audio sources on the basis of specified criteria. Follow these steps to search for a specific Music On Hold audio source in the Cisco Unified Communications Manager database.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note
During your work in a browser session, Cisco Unified Communications Manager Administration retains your Music On Hold audio source search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your Music On Hold audio source search preferences until you modify your search or close the browser.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Procedure

Step 1
Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.
Step 4  From the list of records that display, click the link for the record that you want to view.

<table>
<thead>
<tr>
<th>Note</th>
<th>To reverse the sort order, click the up or down arrow, if available, in the list header.</th>
</tr>
</thead>
</table>

The window displays the item that you choose.

**Additional Information**
See the “Related Topics” section on page 36-36.

### Configuring a Music On Hold Audio Source

Perform the following procedure to add or update a Music On Hold audio source. Use this procedure to associate an existing audio source with an audio stream number or to upload a new custom audio source.

<table>
<thead>
<tr>
<th>Note</th>
<th>If a new version of an audio source file is available, you must perform the update procedure to use the new version.</th>
</tr>
</thead>
</table>

**Procedure**

**Step 1** Choose Media Resources > Music On Hold Audio Source.
The Find and List Music On Hold Audio Sources window displays.

**Step 2** Perform one of the following tasks:
- To add a new Music On Hold audio source, click Add New.
The Music On Hold Audio Source Configuration window displays.
- To update a Music On Hold audio source, locate a specific Music On Hold audio source as described in “Finding a Music On Hold Audio Source” section on page 36-19.

**Step 3** Enter the appropriate settings as described in Table 36-4.

**Step 4** Click Save.
If you added a Music On Hold Audio Source, the list box at the bottom of the window now includes the new Music On Hold audio source.

<table>
<thead>
<tr>
<th>Note</th>
<th>The MOH Audio Source File Status pane tells you about the MOH audio translation status for the added source.</th>
</tr>
</thead>
</table>

**Additional Information**
See the “Related Topics” section on page 36-36.
Deleting a Music On Hold Audio Source

Perform the following procedure to delete an existing Music On Hold audio source.

Note

Deletion does not remove the Music On Hold audio source files. Deletion only removes the association with the MOH Audio Stream number.

Procedure

Step 1  Choose Media Resources > Music On Hold Audio Source.

The Find and List Music On Hold Audio Sources window displays.

Step 2  To locate a specific Music On Hold audio source, enter search criteria and click Find.

A list of Music On Hold audio sources that match the search criteria displays.

Step 3  Perform one of the following actions:

- Check the check boxes next to the Music On Hold audio sources that you want to delete and click Delete Selected.
- Delete all Music On Hold audio sources in the window by clicking Select All and then clicking Delete Selected.
- From the list, choose the name of the Music On Hold audio source that you want to delete and click Delete.

A confirmation dialog displays.

Step 4  Click OK.

The association of the chosen Music On Hold audio source with an audio stream number gets deleted.

Additional Information

See the “Related Topics” section on page 36-36.

Music On Hold Audio Source Configuration Settings

Table 36-4  describes the configuration settings that are used for configuring Music On Hold audio sources.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Music On Hold Audio Source Information</strong></td>
<td></td>
</tr>
<tr>
<td>MOH Audio Stream Number</td>
<td>Use this field to choose the stream number for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays. For existing MOH audio sources, this value displays in the MOH Audio Source title.</td>
</tr>
<tr>
<td>MOH Audio Source File</td>
<td>Use this field to choose the file for this MOH audio source. To do so, click the drop-down arrow and choose a value from the list that displays.</td>
</tr>
</tbody>
</table>
### Table 36-4 Music On Hold Audio Source Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOH Audio Source Name</td>
<td>Enter a unique name in this field for the MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.</td>
</tr>
<tr>
<td>Play continuously (repeat)</td>
<td>To specify continuous play of this MOH audio source, check this check box.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cisco recommends checking this check box. If continuous play of an audio source is not specified, only the first party placed on hold, not additional parties, will receive the MOH audio source.</td>
</tr>
<tr>
<td>Allow Multicasting</td>
<td>To specify that this MOH audio source allows multicasting, check this check box.</td>
</tr>
<tr>
<td>MOH Audio Source File Status</td>
<td>This pane displays information about the source file for a chosen MOH audio source. For an MOH audio source, the following attributes display:</td>
</tr>
<tr>
<td></td>
<td>• InputFileName</td>
</tr>
<tr>
<td></td>
<td>• ErrorCode</td>
</tr>
<tr>
<td></td>
<td>• ErrorText</td>
</tr>
<tr>
<td></td>
<td>• DurationSeconds</td>
</tr>
<tr>
<td></td>
<td>• DiskSpaceKB</td>
</tr>
<tr>
<td></td>
<td>• LowDateTime</td>
</tr>
<tr>
<td></td>
<td>• HighDateTime</td>
</tr>
<tr>
<td></td>
<td>• OutputFileList</td>
</tr>
<tr>
<td></td>
<td>- ULAW wav file name and status</td>
</tr>
<tr>
<td></td>
<td>- ALAW wav file name and status</td>
</tr>
<tr>
<td></td>
<td>- G.729 wav file name and status</td>
</tr>
<tr>
<td></td>
<td>- Wideband wav file name and status</td>
</tr>
<tr>
<td></td>
<td>• Date MOH Audio Translation completed</td>
</tr>
</tbody>
</table>
### Fixed Music On Hold Audio Source Configuration

The music on hold server supports one fixed-device stream source in addition to the file stream sources. This source represents the fixed audio source, which gets configured in the Fixed MOH Audio Source Configuration window. The fixed audio source gets sourced from a fixed device that uses the local computer audio driver.

For each cluster, you may define one fixed audio source. You must set up the fixed audio source that is configured per cluster on each MOH server. To do so, use the Cisco USB MOH sound adapter, which must be ordered separately.

**Note**

The Fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Cisco Unified Communications Manager does not support USB when running on VMware. Internal Music On Hold, however, is supported on VMware.

### Additional Information

See the “Related Topics” section on page 36-36.
Use the following topics to configure the fixed Music On Hold audio source:

- Configuring the Fixed Music On Hold (MOH) Audio Source, page 36-24
- Deleting a Fixed Music On Hold (MOH) Audio Source, page 36-24
- Fixed Music On Hold (MOH) Audio Source Configuration Settings, page 36-25

Configuring the Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to configure the fixed music on hold audio source.

Procedure

**Step 1**  Choose Media Resources > Fixed MOH Audio Source.

The Fixed MOH Audio Source Configuration window displays.

**Step 2**  To configure and enable a fixed music on hold (MOH) audio source, enter the appropriate settings as described in Table 36-5.

**Step 3**  Click Save.

The Fixed MOH Audio Source Configuration window displays an Update Successful status message.

Additional Information

See the “Related Topics” section on page 36-36.

Deleting a Fixed Music On Hold (MOH) Audio Source

Perform the following procedure to delete an existing fixed music on hold audio source.

Procedure

**Step 1**  Choose Media Resources > Fixed MOH Audio Source.

The Fixed MOH Audio Source Configuration window displays.

**Step 2**  If the fixed MOH audio source that displays is enabled (that is, the Enable check box has been checked), you can delete this fixed MOH audio source.

To delete this fixed MOH audio source, click Delete.

A confirmation dialog box displays.

**Step 3**  Click OK.

The chosen fixed music on hold audio source gets deleted from the database.

Additional Information

See the “Related Topics” section on page 36-36.
**Fixed Music On Hold (MOH) Audio Source Configuration Settings**

Table 36-5 describes the configuration settings that are used for configuring the fixed music on hold (MOH) audio source.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed MOH Audio Source Information</td>
<td></td>
</tr>
<tr>
<td>Source ID</td>
<td>This field displays the stream number for this fixed MOH audio source.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name in this field for the fixed MOH audio source.</td>
</tr>
<tr>
<td></td>
<td>This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Cisco Unified Communications Manager does not support USB when running on VMware. Internal Music On Hold, however, is supported on VMware.</td>
</tr>
<tr>
<td>Allow Multicasting</td>
<td>To specify that this fixed MOH audio source allows multicasting, check this check box.</td>
</tr>
<tr>
<td>Enable (If checked, Name is required.)</td>
<td>To enable this fixed MOH audio source, check this check box.</td>
</tr>
</tbody>
</table>

**Additional Information**

See the “Related Topics” section on page 36-36.

**Music On Hold Server Configuration**

You can configure servers for music on hold for a media resource group. Use the following topics to configure music on hold servers:

- Finding a Music On Hold Server, page 36-26
- Configuring a Music On Hold Server, page 36-27
- Resetting or Restarting a Music On Hold Server, page 36-27
- Synchronizing a Music on Hold Server, page 36-28
- Music On Hold Server Configuration Settings, page 36-28

For any music on hold server that you configure, you may trace the configuration of that server. See the Cisco Unified Serviceability Administration Guide for more information.

**Additional Information**

See the “Related Topics” section on page 36-36.
Finding a Music On Hold Server

Because you might have several music on hold servers in your network, Cisco Unified Communications Manager lets you locate specific music on hold servers on the basis of specific criteria. Use the following procedure to locate music on hold servers.

Procedure

Step 1
Choose Media Resources > Music On Hold Server.
The Find and List Music On Hold Servers window displays. Records from an active (prior) query may also display in the window.

Step 2
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3
Click Find.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note
You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4
From the list of records that display, click the link for the record that you want to view.

Note
To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information
See the “Related Topics” section on page 36-36.
Configuring a Music On Hold Server

Perform the following procedure to update a music on hold server.

\textbf{Note} 

You cannot add nor delete a music on hold server.

\textbf{Procedure}

\textbf{Step 1} Choose \textit{Media Resources} > \textit{Music On Hold Server}. The Find and List Music On Hold Servers window displays. Use the two drop-down list boxes to search for a music on hold server.

\textbf{Step 2} To update a music on hold server, click the music on hold server that you want to update. The Music On Hold (MOH) Server Configuration window displays.

\textbf{Step 3} Enter or update the appropriate settings as described in \textit{Table 36-6}.

\textbf{Step 4} To update this music on hold server, click \textit{Save}. The music on hold server gets updated in the database.

\textbf{Additional Information}

See the “Related Topics” section on page 36-36.

Resetting or Restarting a Music On Hold Server

Perform the following procedure to reset an existing music on hold server.

\textbf{Procedure}

\textbf{Step 1} Locate the music on hold server by using the procedure in the “Finding a Music On Hold Server” section on page 36-26.

\textbf{Step 2} Click the music on hold server that you want to reset.

\textbf{Step 3} Click the \textit{Reset} button. A popup window displays an information message.

\textbf{Step 4} After reading the message, click \textbf{Restart} to restart the music on hold server or click \textbf{Reset} to reset the music on hold server.

\textbf{Step 5} To close the popup window, click \textbf{Close}.

\textbf{Additional Information}

See the “Related Topics” section on page 36-36.
Synchronizing a Music on Hold Server

To synchronize a Music on Hold Server with the most recent configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

   The Find and List Music on Hold Servers window displays.

2. Choose the search criteria to use.

3. Click Find.
   The window displays a list of Music on Hold Servers that match the search criteria.

4. Check the check boxes next to the Music on Hold Servers that you want to synchronize. To choose all Music on Hold Servers in the window, check the check box in the matching records title bar.

5. Click Apply Config to Selected.
   The Apply Configuration Information dialog displays.

6. Click OK.

Additional Information
See the “Related Topics” section on page 36-36.

Music On Hold Server Configuration Settings

Table 36-6 describes the configuration settings that are used for configuring music on hold servers.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td>Host Server</td>
<td>For existing music on hold servers, this field serves for display only.</td>
</tr>
<tr>
<td>Music On Hold Server Name</td>
<td>Enter a unique name for the music on hold server in this required field. This name can comprise up to 15 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the music on hold server. This description can comprise up to 50 characters. Ensure Description does not contain ampersand (&amp;), double quotes (&quot;), brackets ([]), less than (&lt;), greater than (&gt;), or the percent sign (%).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Use this required field to choose a device pool for the music on hold server. To do so, click the drop-down arrow and choose a device pool from the list that displays.</td>
</tr>
</tbody>
</table>
Chapter 36  Music On Hold

Configuring Music On Hold

Location

Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.

From the drop-down list box, choose the appropriate location for this MOH server.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this MOH server consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 or SIP protocol.

To configure a new location, use the System > Location menu option.

For more details about locations, see “Location Configuration” in the Cisco Unified Communications Manager Administration Guide. For an explanation of location-based CAC across intercluster trunks, see “Location-Based Call Admission Control Over Intercluster Trunk” in the Cisco Unified Communications Manager System Guide.

Table 36-6  Music On Hold Server Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this MOH server. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this MOH server consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 or SIP protocol. To configure a new location, use the System &gt; Location menu option. For more details about locations, see “Location Configuration” in the Cisco Unified Communications Manager Administration Guide. For an explanation of location-based CAC across intercluster trunks, see “Location-Based Call Admission Control Over Intercluster Trunk” in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Maximum Half Duplex Streams</td>
<td>Enter a number in this required field for the maximum number of unicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on unicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 0 to 500.</td>
</tr>
<tr>
<td>Maximum Multicast Connections</td>
<td>Enter a number in this required field for the maximum number of multicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on multicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 1 to 999999.</td>
</tr>
<tr>
<td>Fixed Audio Source Device</td>
<td>Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.</td>
</tr>
</tbody>
</table>
Chapter 36      Music On Hold

Configuring Music On Hold

Location Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location.

From the drop-down list box, choose the appropriate location for this MOH server.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this MOH server consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 or SIP protocol.

To configure a new location, use the System > Location menu option.

For more details about locations, see “Location Configuration” in the Cisco Unified Communications Manager Administration Guide. For an explanation of location-based CAC across intercluster trunks, see “Location-Based Call Admission Control Over Intercluster Trunk” in the Cisco Unified Communications Manager System Guide.

Maximum Half Duplex Streams Enter a number in this required field for the maximum number of unicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on unicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 0 to 500.

Maximum Multicast Connections Enter a number in this required field for the maximum number of multicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on multicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 1 to 999999.

Fixed Audio Source Device Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this MOH server. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this MOH server consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 or SIP protocol. To configure a new location, use the System &gt; Location menu option. For more details about locations, see “Location Configuration” in the Cisco Unified Communications Manager Administration Guide. For an explanation of location-based CAC across intercluster trunks, see “Location-Based Call Admission Control Over Intercluster Trunk” in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Maximum Half Duplex Streams</td>
<td>Enter a number in this required field for the maximum number of unicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on unicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 0 to 500.</td>
</tr>
<tr>
<td>Maximum Multicast Connections</td>
<td>Enter a number in this required field for the maximum number of multicast music on hold streams that this music on hold server supports. This value determines the maximum number of devices that can be on multicast music on hold that is streamed from this music on hold server at any given time. Valid values range from 1 to 999999.</td>
</tr>
<tr>
<td>Fixed Audio Source Device</td>
<td>Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.</td>
</tr>
</tbody>
</table>
Configuring Music On Hold

Use Trusted Relay Point

From the drop-down list box, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- Off—Choose this value to disable the use of a TRP with this device.
- On—Choose this value to enable the use of a TRP with this device.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent).

If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the “TRP Insertion in Cisco Unified Communications Manager” section in the Cisco Unified Communications Manager System Guide for details of call behavior.

If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP.

See the “Trusted Relay Point” section and its subtopics in the “Media Resource Management” chapter of the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

Run Flag

Use this required field to choose a run flag for the music on hold server. To do so, click the drop-down arrow and choose Yes or No. Choosing No disables the music on hold server.

Enable Multicast Audio Sources on this MOH Server

Check or uncheck this check box to enable or disable multicast of audio sources for this music on hold server.

Note: If this MOH server belongs to a multicast media resource group, a message asks you to enable multicast on this MOH server or to update the specified media resource group(s) either by removing this MOH server or by changing the multicast setting of each listed group.
Table 36-6  Music On Hold Server Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Base Multicast IP Address | If multicast support is needed, enter the base multicast IP address in this field. Valid IP addresses for multicast range from 224.0.1.0 to 239.255.255.255.  
  Note  IP addresses between 224.0.1.0 and 238.255.255.255 fall in the reserved range of IP multicast addresses for public multicast applications. Use of such addresses may interfere with existing multicast applications on the Internet. Cisco strongly recommends using IP addresses in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 - 239.255.255.255). |
| Base Multicast Port Number | If multicast support is needed, enter the base multicast port number in this field. Valid multicast port numbers include even numbers that range from 16384 to 32766. |
| Increment Multicast on | Click **Port Number** to increment multicast on port number.  
  Click **IP Address** to increment multicast on IP address.  
  Note  Use multicast by incrementing IP address as the preferred method in firewall situations. This results in a unique IP address for each multicast audio source and helps to avoid network saturation. |

**Selected Multicast Audio Sources**

- Only audio sources for which the Allow Multicasting check box was checked display in this listing. If no such audio sources exist, the following message displays:  
  - There are no Music On Hold Audio Sources selected for Multicasting. Click Configure Audio Sources in the top right corner of the page to select Multicast Audio Sources.  
  - From the Related Links drop-down list box, choose Configure Audio Sources and click **Go**.  
- **No.** This field designates music on hold audio stream number that is associated with a particular multicast audio source. Only audio sources that are defined as allowing multicasting display.  
- **Audio Source Name** This field designates name of audio source that is defined as allowing multicasting.  
- **Max Hops** For each multicast audio source, enter the maximum number of router hops through which multicast packets should pass. Valid values range from 1 to 127.  
  Note  Using high values can lead to network saturation. This field also gets identified as **Time to Live**.

**Additional Information**

See the “Related Topics” section on page 36-36.
Music On Hold Audio File Management Configuration

You can manage the audio files that the Music On Hold feature uses as audio sources. The Media Resources > MOH Audio File Management menu option allows the administrator to perform the following functions:

- Display a list of the MOH audio files that are stored on the system.
- Upload new MOH audio files.
- Delete MOH audio files.

Use the following topics to manage the music on hold audio source audio files:

- Displaying Music On Hold Audio Files, page 36-33
- Uploading a Music On Hold Audio File, page 36-34
- Deleting a Music On Hold Audio File, page 36-35

Additional Information
See the “Related Topics” section on page 36-36.

Displaying Music On Hold Audio Files

Use the following procedure to display a list of music on hold audio files that are stored on the system.

Procedure

Step 1  In Cisco Unified Communications Manager Administration, choose Media Resources > MOH Audio File Management.

The Music On Hold Audio File Management window displays.

For each entry in the list of records, the following information displays:

- Check box—If the audio file can be deleted, a check box displays in the first column of the display.
- File Name—This column displays the audio file name.
- Length—This column displays the audio file length in minutes and seconds.
- File Status—This column displays the file status, including the following values:
  - Translation Complete—Files with this status uploaded successfully and are available for use as audio files for a music on hold audio source.
  - In Use—After you add a music on hold audio source that uses this audio file as its MOH audio source file, the file status for this audio file changes to In Use. You cannot delete files with this file status.

Additional Information
See the “Related Topics” section on page 36-36.
Uploading a Music On Hold Audio File

Perform the following procedure to upload a music on hold audio file. Uploading the audio file makes it available for use as a music on hold audio source. If you use the Media Resources > Music On Hold Audio Source menu option to add a new audio source, the addition makes the newly uploaded audio file available in the MOH Audio Source File drop-down list box.

Procedure

Step 1
Choose Media Resources > MOH Audio File Management.
The Music On Hold Audio File Management window displays.

Step 2
Click the Upload File button.
The Upload File popup window displays.

Step 3
Choose one of the following options:
- If you know the path to a file that specifies an audio file, enter the path in the File field.
- If you do not know the path and file name, search for the audio file by clicking the Browse... button to the right of the File field. After you find the audio file, click the desired audio file and click Open. The path to the chosen audio file displays in the File field of the Upload File popup window.

Step 4
To upload the specified audio file, click Upload.
After the audio file gets uploaded, the Upload Result window tells you the result of the upload.

Note
Uploading a file uploads the file to the Cisco Unified Communications Manager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete.

Note
Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco Unified Communications Manager Administration on each server. MOH audio source files do not automatically propagate to other MOH servers in a cluster.

Step 5
To close the Upload Result window, click Close.
The newly uploaded audio file gets added to the list of audio files in the MOH Audio File Management window.

Additional Information
See the “Related Topics” section on page 36-36.
Deleting a Music On Hold Audio File

Perform the following procedure to delete an existing music on hold audio file.

**Note**
You cannot delete MOH audio files that specify the *In Use* state. To delete such files, first use the *Media Resources > Music On Hold Audio Source* menu option to find MOH audio sources that use this audio file. Either delete those MOH audio sources or modify them, so they use a different audio file.

**Procedure**

**Step 1**
Choose *Media Resources > MOH Audio File Management*.
The Music On Hold Audio File Management window displays.

**Step 2**
Click the check box to the left of a music on hold audio file that you want to delete.

**Note**
You can click several audio files to delete multiple audio files at once. You can also click the *Select All* button to select all audio files for deletion. Use the *Clear All* button to deselect audio files that you have selected.

**Step 3**
Click the *Delete Selected* button.
A popup window warns that this file will be deleted permanently.

**Step 4**
To complete the deletion, click *OK*.
The audio file gets deleted from the list of music on hold audio files.

**Additional Information**
See the “Related Topics” section on page 36-36.
Viewing Music On Hold Server Performance

To view music on hold server perfmon counters, use the Cisco Unified Real Time Monitoring Tool (RTMT).

Table 36-7 details the performance monitoring counters that display in the Cisco Unified Real Time Monitoring Tool Performance window.

<table>
<thead>
<tr>
<th>Performance Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOHConnectionState</td>
<td>Indicates primary and secondary Cisco Unified Communications Manager:</td>
</tr>
<tr>
<td></td>
<td>• 1 = Primary</td>
</tr>
<tr>
<td></td>
<td>• 2 = Secondary</td>
</tr>
<tr>
<td></td>
<td>• 0 = Not connected</td>
</tr>
<tr>
<td>MOHAudioSourcesActive</td>
<td>Specifies total number of active audio sources, including each supported codec type. If audio Source 1 has mu-law and G.729 enabled, count for this audio source may show 2.</td>
</tr>
<tr>
<td>MOHStreamsActive</td>
<td>Specifies total number of active streams. Two potential overhead streams exist for each audio source/codec type: one for actual audio source, another for multicast.</td>
</tr>
<tr>
<td>MOHStreamsAvailable</td>
<td>Specifies total number of available simplex streams. Total represents total number of streams that are available in device driver for all devices.</td>
</tr>
<tr>
<td>MOHConnectionsLost</td>
<td>Specifies number of times that connection has been lost for the corresponding Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>MOHStreamsTotal</td>
<td>Specifies total number of streams that are processed.</td>
</tr>
</tbody>
</table>

Checking Service States

To check whether the music on hold service is running, use Performance Management.

Additional Information

See the “Related Topics” section on page 36-36.

Related Topics

- Configuration Checklist for Music On Hold, page 36-1
- Configuration Checklist for Multicast, page 36-3
- Configuration Checklist for Monitoring Music On Hold Performance, page 36-4
- Introducing Music On Hold, page 36-4
- Music On Hold Definitions, page 36-4
- Music On Hold Characteristics, page 36-6
• Music On Hold Functionality, page 36-7
• Supported Music On Hold Features, page 36-8
• Music On Hold System Requirements and Limits, page 36-16
• Music On Hold Failover and Fallback, page 36-18
• Media Resource Group Configuration, Cisco Unified Communications Manager Administration Guide
• Media Resource Group List Configuration, Cisco Unified Communications Manager Administration Guide

Music On Hold Audio Sources
• Music On Hold Audio Sources, page 36-12
• Storing Audio Source Files, page 36-12
• Managing Audio Sources, page 36-13
• Multicast and Unicast Audio Sources, page 36-13
• Multicast Music On Hold Over H.323 Intercluster Trunks, page 36-15
• Configuration Checklist for Multicast, page 36-3
• Finding a Music On Hold Audio Source, page 36-19
• Configuring a Music On Hold Audio Source, page 36-20
• Deleting a Music On Hold Audio Source, page 36-21
• Music On Hold Audio Source Configuration Settings, page 36-21

Fixed Music On Hold Audio Source
• Fixed Music On Hold Audio Source Configuration, page 36-23
• Configuring the Fixed Music On Hold (MOH) Audio Source, page 36-24
• Deleting a Fixed Music On Hold (MOH) Audio Source, page 36-24
• Fixed Music On Hold (MOH) Audio Source Configuration Settings, page 36-25

Music On Hold Servers
• Music On Hold Server, page 36-11
• Checking Service States, page 36-36
• Music On Hold Server Configuration, page 36-25
• Finding a Music On Hold Server, page 36-26
• Configuring a Music On Hold Server, page 36-27
• Resetting or Restarting a Music On Hold Server, page 36-27
• Synchronizing a Music on Hold Server, page 36-28
• Music On Hold Server Configuration Settings, page 36-28
• Trusted Relay Point, Cisco Unified Communications Manager System Guide

Music On Hold Audio File Management
• Music On Hold Audio File Management Configuration, page 36-33
• Displaying Music On Hold Audio Files, page 36-33
Related Topics

- Uploading a Music On Hold Audio File, page 36-34
- Deleting a Music On Hold Audio File, page 36-35

Additional Cisco Documentation

- Internet Protocol Version 6 (IPv6), page 29-1
- Cisco Unified Real Time Monitoring Tool Administration Guide
- Installing Cisco Unified Communications Manager Release 8.5(1)
- Upgrading Cisco Unified Communications Manager Release 8.5(1)
- Cisco Unified Serviceability Administration Guide
Presence

The Presence feature allows a user to monitor the real-time status of another user at a directory number or SIP URI.

This section covers the following topics:
- Configuration Checklist for Presence, page 37-1
- Introducing Presence, page 37-4
- Understanding How Presence Works with Phones and Trunks, page 37-5
- Understanding How Presence Works with Route Lists, page 37-6
- Understanding Presence Groups, page 37-7
- Understanding Presence Authorization, page 37-9
- Understanding How the SUBSCRIBE Calling Search Space Works, page 37-11
- System Requirements, page 37-12
- Presence Feature Interactions/Restrictions, page 37-12
- Configuring Presence, page 37-13
- Related Topics, page 37-22

Configuration Checklist for Presence

The Presence feature allows a user (watcher) to monitor the real-time status of another user at a directory number or SIP URI from the device of the watcher. A watcher can monitor the status of the user by using the following options:
- BLF/SpeedDial buttons
- Missed call, placed call, or received call lists in the directories window
- Shared directories, such as the corporate directory

Tip

The following information assumes that the phones and SIP trunks exist in the Cisco Unified Communications Manager database. For information on how to add a phone or SIP trunk, see the Cisco Unified Communications Manager Administration Guide.
Table 37-1 provides tasks that you must perform to configure presence features:

- To configure the call list phone feature for presence, perform Step 2 through Step 7.
- To configure the BLF/SpeedDial phone feature for presence, perform Step 3 and Step 6 through Step 10.

**Note**

You do not need to configure presence groups or the Default Inter-Presence Group Subscription parameter for BLF/SpeedDials.

- To configure both features, perform all the steps in the checklist.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you have not already done so, configure the phones and SIP trunks that you plan to use with the presence feature.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enable the BLF for Call Lists enterprise parameter.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configure the clusterwide service parameters for presence in Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>To use presence group authorization, configure presence groups and permissions.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Apply a presence group to the directory number, SIP trunk, phone that is running SIP, phone that is running SCCP, end user, and application user (for application users that are sending presence requests over the SIP trunk) in Cisco Unified Communications Manager Administration.</td>
</tr>
</tbody>
</table>
### Table 37-1 Presence Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Procedures and Related Topics</th>
</tr>
</thead>
</table>
| **Step 6** | To allow presence requests from a SIP trunk, check the **Accept Presence Subscription** check box in the SIP Trunk Security Profile Configuration window.  
To enable application-level authorization for a SIP trunk application in addition to trunk-level authorization, check the following check boxes in the SIP Trunk Security Profile Configuration window:  
- Enable Digest Authentication  
- Enable Application Level Authorization  
**Note** You cannot check Enable Application Level Authorization unless Enable Digest Authentication is checked.  
Apply the profile to the trunk. Reset the trunk for the changes to take effect.  
If you checked Enable Application Level Authorization, check the Accept Presence Subscription check box in the Application User Configuration window for the application. |
| **Step 7** | Configure the SUBSCRIBE Calling Search Space and apply the calling search space to the phone, trunk, or end user, if required.  
Understanding How the SUBSCRIBE Calling Search Space Works, page 37-11  
Configuring and Applying the SUBSCRIBE Calling Search Space, page 37-14  
Calling Search Space Configuration, Cisco Unified Communications Manager Administration Guide  
Understanding How Presence Works with Route Lists, page 37-6 |
| **Step 8** | Customize phone button templates for the BLF/SpeedDial buttons.  
Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, page 37-20 |
| **Step 9** | If you have not already done so, configure the phone where you want to add the BLF/SpeedDial buttons; make sure that you choose the phone button template that you configured for the BLF/SpeedDial lines.  
Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide |
| **Step 10** | Introducing Presence, page 37-4  
Understanding How Presence Works with Phones and Trunks, page 37-5  
Configuring BLF/SpeedDial Buttons, page 37-20  
BLF/SpeedDial Configuration Settings, page 37-21 |
Introducing Presence

When you configure Presence in Cisco Unified Communications Manager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI, a presence entity, from the device of the watcher.

A SIP URI comprises a call destination configured with a user@host format, such as xten3@CompB.cisco.com or 2085017328@10.21.91.156:5060.

A watcher can monitor the status of the presence entity (also called presentity) with the following options:

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

Call lists and directories display the BLF status for existing entries. When you configure BLF/SpeedDial buttons, the presence entity displays as a speed dial on the device of the watcher.

For presence-supported phones that are running SIP, you can configure directory numbers or SIP URIs as BLF/SpeedDial buttons. For presence-supported phones that are running SCCP, you can only configure directory numbers as BLF/SpeedDial buttons.

You configure BLF/SpeedDial buttons for a phone or user device profile. The BLF value does not have to be on the cluster. For information on the Busy Lamp Field (BLF) status icons that display on the phone, see the Cisco Unified IP Phone documentation that supports your phone. To identify whether your phone supports presence, see the Cisco Unified IP Phone documentation that supports your phone and this version of Cisco Unified Communications Manager.

To view the status of a presence entity, watchers send presence requests to Cisco Unified Communications Manager. After administrators configure presence features, real-time status icons display on the watcher device to indicate whether the presence entity is on the phone, not on the phone, status unknown, and so on.

Extension mobility users can use presence features on phones with extension mobility support.

Presence group authorization ensures that only authorized watchers can access the presence status for a destination. Because the administrator ensures that the watcher is authorized to monitor the destination when a BLF/Speed Dial is configured, presence group authorization does not apply to BLF/Speed Dials.

For phones that are running SIP, presence group authorization also does not apply to any directory number or SIP URI that is configured as a BLF/Speed Dial that appears in a call list.

To allow presence requests from outside the cluster, administrators must configure the system to accept presence requests from the external trunk or application. You can assign presence groups to trunks and applications outside the cluster to invoke presence group authorization.

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes presence requests that come from the trunk or the phone. The SUBSCRIBE Calling Search Space that is associated with an end user gets used for extension mobility calls.
Understanding How Presence Works with Phones and Trunks

Use the information in this section with the “Understanding Presence Groups” section on page 37-7, the “Understanding Presence Authorization” section on page 37-9, the “Understanding How Presence Works with Route Lists” section on page 37-6, and the “Understanding How the SUBSCRIBE Calling Search Space Works” section on page 37-11. The following information assumes that the phones and trunks have permission to view the status of the presence entity, as configured through presence groups.

Cisco Unified Communications Manager handles all presence requests for Cisco Unified Communications Manager users, whether inside or outside the cluster.

For a Cisco Unified Communications Manager watcher that sends a presence request through the phone, Cisco Unified Communications Manager responds with the presence status directly if the phone and presence entity are colocated.

If the device exists outside of the cluster, Cisco Unified Communications Manager queries the external device through the SIP trunk. If the watcher has permission to monitor the external device, the SIP trunk sends the presence request to the external device and returns presence status to the watcher.

For non-Cisco Unified Communications Manager watchers that send presence requests through a Cisco Unified Communications Manager trunk, Cisco Unified Communications Manager responds with presence status if Cisco Unified Communications Manager supports the presence entity. If Cisco Unified Communications Manager does not support the presence entity, the request gets rejected.

The following examples demonstrate how presence works for phones and trunks when the phones and trunks have permission to send and receive presence requests.

**A Cisco Unified Communications Manager User Queries the BLF Status of Another Cisco Unified Communications Manager User.**

A Cisco Unified Communications Manager user calls another Cisco Unified Communications Manager user only to find that the called party is not available. When available, the called party checks the missed call list, and the phone contacts Cisco Unified Communications Manager. Cisco Unified Communications Manager validates that the called party is a valid watcher and determines that the caller represents a Cisco Unified Communications Manager presence entity. The BLF status for the caller gets updated on the phone of the called party.

**A Cisco Unified Communications Manager User Queries the BLF Status of a Non-Cisco Unified Communications Manager User.**

A non-Cisco Unified Communications Manager user calls a Cisco Unified Communications Manager user only to find that the Cisco Unified Communications Manager user is unavailable. When available, the Cisco Unified Communications Manager user checks the missed call list, and the phone contacts Cisco Unified Communications Manager. Cisco Unified Communications Manager confirms that the Cisco Unified Communications Manager user is a valid watcher and determines that the non-Cisco Unified Communications Manager user represents a presence entity. A SIP trunk interacts with the non-Cisco Unified Communications Manager network and Cisco Unified Communications Manager, and status for the non-Cisco Unified Communications Manager user gets updated on the phone of the Cisco Unified Communications Manager user.
A Non-Cisco Unified Communications Manager User Queries the Presence Status of a Cisco Unified Communications Manager User.

A non-Cisco Unified Communications Manager user queries the state of a Cisco Unified Communications Manager user. The request comes through a Cisco Unified Communications Manager SIP trunk. Cisco Unified Communications Manager verifies that the non-Cisco Unified Communications Manager user is a valid watcher and determines that the Cisco Unified Communications Manager user represents a Cisco Unified Communications Manager presence entity. Cisco Unified Communications Manager sends the status to phone of the non-Cisco Unified Communications Manager user.

A Cisco Unified Communications Manager Accesses the Corporate Directory to Get BLF Status.

A Cisco Unified Communications Manager user accesses the corporate directory on the phone. For each directory entry, BLF status displays.

A Phone Monitors a BLF/SpeedDial.

After an administrator configures the presence feature and the BLF/SpeedDial buttons, a user can immediately begin to monitor the real-time status of a presence entity.

Understanding How Presence Works with Route Lists

Use the information in this section with the “Understanding How Presence Works with Phones and Trunks” section on page 37-5, the “Understanding Presence Groups” section on page 37-7, the “Understanding Presence Authorization” section on page 37-9, and the “Understanding How the SUBSCRIBE Calling Search Space Works” section on page 37-11.

Cisco Unified Communications Manager receives presence requests from watchers and status responses from presence entities. Watchers and presence entities can exist inside the cluster or outside of the cluster.

Cisco Unified Communications Manager supports external incoming and outgoing presence requests through the SIP trunk. SIP trunks can be members of route groups, which are members of route lists. When Cisco Unified Communications Manager receives a presence request or notification status that is associated with an outbound SIP trunk or route group, Cisco forwards the request or status to a SIP trunk.

Presence requests and responses must route to SIP trunks or routes that are associated with SIP trunks. The system rejects presence requests routing to MGCP/H323 trunk devices.

When a request gets forwarded to a route group or list, any SIP trunk in the group or list can carry the request. Cisco Unified Communications Manager forwards the request to the next available or idle outbound SIP trunk in the group or list. This process repeats until Cisco Unified Communications Manager receives a successful response or the operation fails.

After the presence request to an external presentity is successful, the SIP trunk receives notification messages based on status changes for the presentity and sends the status to the route list/group to notify the watcher. When different watchers send presence requests to the same presentity that is reached through the route list/group and SIP trunk, Cisco Unified Communications Manager sends the cached status for the presentity to the subscriber instead of creating another subscription.
The presentity can terminate the subscription at any time due to time-out or other reasons. When the SIP trunk receives a termination status, the termination status gets passed to the route list or group to notify the watcher.

See the “Route List Configuration” chapter in the Cisco Unified Communications Manager Administration Guide for more information about configuring route lists.

Understanding Presence Groups

Tip

The Default Inter-Presence Group Subscription service parameter for the Cisco CallManager service sets the clusterwide permissions parameter for presence groups to Allow Subscription or Disallow Subscription. This enables administrators to set a system default and configure presence group relationships by using the default setting for the cluster. For information on configuring this service parameter, see the “Configuring Presence Service Parameters and Enterprise Parameters” section on page 37-13.

Cisco Unified Communications Manager allows you to configure presence groups to control the destinations that watchers can monitor. To configure a presence group, create the group in Cisco Unified Communications Manager Administration and assign one or more destinations and watchers to the same group.

Note

The system always allows presence requests within the same presence group.

You must also specify the relationships to other presence groups by using one of the following permissions from the drop-down list in the Presence Group Configuration window:

- **Use System Default**—To use the Default Inter-Presence Group Subscription service parameter (Allow Subscription or Disallow Subscription) setting for the permission setting, select the group(s) and configure the Subscription Permission to Use System Default.
- **Allow Subscription**—To allow a watcher in this group to monitor members in another group, select the group(s) and configure the Subscription Permission setting to Allow Subscription.
- **Disallow Subscription**—To block a watcher in this group from monitoring members in another group, select the group(s) and configure the Subscription Permission setting to Disallow Subscription.

Tip

Whenever you add a new presence group, Cisco Unified Communications Manager defines all group relationships for the new group with the default cluster setting as the initial permission setting. To apply different permissions, you configure new permissions between the new group and existing groups for each permission that you want to change.

The permissions that are configured for a presence group display in the Presence Group Relationship pane. Permissions that use the system default permission setting for the group-to-group relationship do not display.
Example: Configuring Presence Group Permissions

Assume the clusterwide setting for Default Inter-Presence Group Subscription is set to Disallow Subscription. You create two presence groups: Group A (workers) and Group B (managers). If you want to allow Group B members to monitor Group A members but to block group A members from monitoring Group B members, you would configure Allow Subscription for Group B to Group A. (Because the system default is Disallow Subscription, Group A already disallows subscriptions to Group B, unless you change the Default Inter-Presence Group Subscription service setting.)

Cisco Unified Communications Manager automatically creates the Standard Presence Group at installation, which serves as the default group for presence users. All presence users (except application user) initially get assigned to the Standard Presence group. You cannot delete this group.

Note

Because not all application users use the SIP trunk or initiate presence requests, the default setting for application user specifies None. To assign an application user to the Standard Presence Group, administrators must configure this option.

For each presence group that you create, you apply the presence group to one or more of following items in Cisco Unified Communications Manager Administration (see Table 37-2).

Table 37-2 Applying Presence Groups

<table>
<thead>
<tr>
<th>Apply Presence Groups to</th>
<th>Presence Entity or Watcher</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory number</td>
<td>Presence entity</td>
<td>For phones that are running either SIP or SCCP</td>
</tr>
<tr>
<td>Trunk</td>
<td>Watcher and Presence Entity</td>
<td>For external presence servers that send presence requests via SIP trunk or a proxy server that is connected on SIP trunk (serving as watcher) For outgoing presence requests to the SIP trunk (serving as presence entity)</td>
</tr>
<tr>
<td>Phone</td>
<td>Watcher</td>
<td>For phones that are running either SIP or SCCP</td>
</tr>
<tr>
<td>Application User</td>
<td>Watcher</td>
<td>For external applications that send presence requests via SIP trunk or home on a proxy server that is connected on SIP trunk (for example Web Dial, IPPM, Meeting Place, conference servers, and presence servers)</td>
</tr>
<tr>
<td>End User</td>
<td>Watcher</td>
<td>For user directories and call lists and to configure extension mobility settings.</td>
</tr>
</tbody>
</table>

Note 1: A phone serves as a watcher; a line on a phone cannot serve as a watcher.

Note 2: You do not need to provision presence groups for BLF/SpeedDials.
Chapter 37        Presence

Understanding Presence Authorization

Tip

See the “Understanding Presence Authorization” section on page 37-9, for additional requirements for presence requests through the SIP trunk.

The following examples describe how a phone or trunk obtains the destination status by using different presence groups and permissions.

A Phone Wants Status About a Directory Number That Is Assigned to BLF/SpeedDial.

Phone A, which is colocated with Phone B, has directory number 1111 (Phone B) that is configured as a BLF/SpeedDial button to monitor presence status for Phone B. Phone A receives real-time status for directory number 1111 and displays the status icon next to the BLF/SpeedDial button. The system does not invoke presence group authorization.

A Phone Wants Status About a Directory Number in a Call List.

Phone A, which has the presence group, User Group, that is configured for it, has directory number 1111 in the Missed Calls call list. Directory number 1111, which exists for Phone B, has the presence group, Executive Group, that is configured for it. The Presence Group Configuration window indicates that the relationship between the User Group and Executive Group is Disallow Subscription, as specified in the Presence Group Relationship pane. Phone A cannot receive real-time status for directory number 1111, and Phone A does not display the real-status icon next to the Missed Call list entry.

A SIP Proxy Server That Is Connected to a SIP Trunk Wants Status About a Cisco Unified Communications Manager Directory Number.

The following example describes how a SIP trunk obtains the status of a directory number when different presence groups are configured for the SIP trunk and directory number. SIP proxy server D uses SIP trunk C to contact Cisco Unified Communications Manager for the status of directory number 5555 because directory number 5555 exists as a BLF/SpeedDial button on phone E that is running SIP, which connects to the proxy server. The SIP trunk indicates that it has presence group, Administrator Group, that is configured for it, and directory number 5555 is assigned to the Engineering Group. The Presence Group Configuration window indicates that the relationship between the Administrator Group and Engineering Group is allowed, as specified in the Presence Group Relationship pane. Cisco Unified Communications Manager sends the status of the directory number to the trunk, which passes the status to the SIP proxy server D. Phone E that is running SIP receives real-time status for directory number 5555, and the phone displays the real-time status icon next to the BLF/SpeedDial button.

Understanding Presence Authorization

Tip

Use the information in this section with the “Understanding How Presence Works with Phones and Trunks” section on page 37-5, the “Understanding Presence Groups” section on page 37-7, and the “Understanding How the SUBSCRIBE Calling Search Space Works” section on page 37-11.

To view the status of a presence entity, watchers send presence requests to Cisco Unified Communications Manager. The system requires watchers to be authorized to initiate status requests for a presence entity by using these mechanisms:

- The watcher presence group must possess authorization to obtain the status for the presence entity presence group, whether inside or outside of the cluster.
Understanding Presence Authorization

- Cisco Unified Communications Manager must possess authorization to accept presence requests from an external presence server or application.

**Note**

The authorization process remains independent of calling search space routing for presence requests.

To initiate presence group authorization, you must configure one or more presence groups and assign the appropriate permissions. Administrators configure permission settings for presence groups, which specify when a presence group for a watcher can monitor the status of members in other groups. To validate a presence request, Cisco Unified Communications Manager performs a database lookup by using the permissions that are assigned to the presence groups that are configured.

If you choose not to use presence group authorization, leave all presence users assigned to the default presence group and do not configure additional groups or permissions. You will still need to configure authorization for a SIP trunk or application if you want to authorize Cisco Unified Communications Manager to accept incoming presence requests from an external presence server or application.

**Tip**

When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.

Administrators configure the Cisco Unified Communications Manager system to accept presence requests that come via the SIP trunk by configuring parameters for the SIP trunk and application user.

To authorize the Cisco Unified Communications Manager system to accept incoming presence requests from the SIP trunk, check the Accept Presence Subscription check box in the SIP Trunk Security Profile Configuration window. (To block incoming presence requests on a SIP trunk, uncheck the check box.) When SIP trunk presence requests are allowed, Cisco Unified Communications Manager accepts requests from the SIP user agent (SIP proxy server or external presence server) that connects to the trunk.

Consider digest authentication as optional when Cisco Unified Communications Manager is configured to accept presence requests from a SIP trunk.

**Tip**

To use presence group authorization with incoming presence requests on a SIP trunk, configure a presence group for the trunk, such as External_Presence_Serv_Group1, and configure the appropriate permissions to other groups inside the cluster.

To authorize the Cisco Unified Communications Manager system to accept presence requests from an external application that connects on the SIP trunk, check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration window and the Accept Presence Subscription check box in the Applications User Configuration window for the application. When you configure the Cisco Unified Communications Manager system to accept presence requests from an application user, Cisco Unified Communications Manager validates each presence request that is received on the SIP trunk before accepting it.

**Tip**

To use presence group authorization with incoming presence requests from a SIP trunk application, configure a presence group for the application, such as Presence_User, and configure the appropriate permissions to other groups inside the cluster.

If you configure both levels of authorization for SIP trunk presence requests, the presence group for the SIP trunk gets used only when no presence group is identified in the incoming request for the application.
Before application authorization can occur, Cisco Unified Communications Manager must first authenticate the external application by using digest authentication. Enable Application Level Authorization cannot be checked unless Enable Digest Authentication is checked.

Note

The authorization could pass for the trunk but fail for the application. See the “Presence Group and Presence Authorization Tips” section on page 37-19, for additional considerations when configuring presence authorization.

See the *Cisco Unified Communications Manager Security Guide* for more information about authentication and authorization.

### Understanding How the SUBSCRIBE Calling Search Space Works

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes presence requests that come from the trunk or the phone. The SUBSCRIBE calling search space, which is associated with a watcher, specifies the list of partitions to search for routing information to a presence entity for presence requests.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (Call Routing > Class of Control > Calling Search Space). For information on how to configure a calling search space, see the “Calling Search Space Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

The SUBSCRIBE Calling Search space option allows you to apply a calling search space separate from the call-processing Calling Search Space for presence requests. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

You apply the SUBSCRIBE Calling Search Space to the SIP trunk, phone, or end user. The SUBSCRIBE Calling Search Space that is associated with an end user gets used for extension mobility calls.

### Understanding How Presence Works with Extension Mobility

Tip

Use the information in this section in conjunction with the “Understanding Presence Groups” section on page 37-7, the “Understanding Presence Authorization” section on page 37-9, and the “Understanding How the SUBSCRIBE Calling Search Space Works” section on page 37-11.

When you configure BLF/SpeedDial buttons in a user device profile in Cisco Unified Communications Manager Administration, a phone that supports Cisco Extension Mobility can display presence status on the BLF/SpeedDial buttons after you log in to the device. The SUBSCRIBE calling search space and presence group that are configured for the user apply.
When the extension mobility user logs out, a phone that supports Cisco Extension Mobility displays presence status on the BLF/SpeedDial buttons for the log-out profile that is configured. When a user device profile is configured for the logout profile, the SUBSCRIBE calling search space and presence group that are configured for the user apply.

Tip
See “Device Profile Configuration” in the Cisco Unified Communications Manager Administration Guide for more information about configuring device profiles.

System Requirements

The following system requirements exist for the Presence feature in Cisco Unified Communications Manager:

- Cisco Unified Communications Manager 8.0(2) (or higher) on each server in the cluster
- To identify the Cisco Unified IP Phone models that support presence or Busy Lamp Field (BLF), generate the Unified CM Phone Features List report in Cisco Unified Reporting. To generate the report, choose BLF Speed Dial, BLF Speed Dial with URI, or Presence Subscription.

Presence Feature Interactions/Restrictions

The following interactions and restrictions apply to the Presence feature:

- Cisco Unified Communications Manager Assistant does not support SIP presence.
- Cisco Unified Communications Manager supports an inbound presence request to a directory number that is associated with a hunt list.
- Cisco Unified Communications Manager rejects presence requests to a directory number that is associated with a hunt pilot.
- The BLF on call list feature is not supported on the Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7960.
- Because the administrator ensures that the watcher is authorized to monitor the destination when configuring a BLF/SpeedDial, presence group authorization does not apply to BLF/SpeedDials. For phones that are running SIP, presence group authorization also does not apply to any directory number or SIP URI that is configured as a BLF/Speed Dial that appears in a call list.
- For Cisco Unified IP Phones with multiple lines, the phone uses the cached information that is associated with the line directory number for missed and placed calls to determine presence authorization. If this call information is not present, the phone uses the primary line as the subscriber for presence authorization. For BLF/SpeedDial buttons on Cisco Unified IP Phones with multiple lines, the phone uses the first available line as the subscriber.
- When a user monitors a directory number that is configured for Cisco Unified IP Phones 7960, 7940, 7905, and 7912 that are running SIP, the system displays a status icon for ‘not on the phone’ on the watcher device when the presentity is off hook (but not in a call connected state). These phones do not detect an off hook status. For all other phone types, the system displays the status icon for ‘on the phone’ on the watcher device for an off-hook condition at the presentity.
- You can configure BLF in the BAT phone template.
The following restrictions apply to Presence BLF interaction with DNs on H.323 phones when the H.323 phone device serves as presentity:

- When the H.323 phone is in the RING IN state, the BLF status gets reported as Busy. (For phone presentities of phones that are running either SCCP or SIP and that are in the RING IN state, the BLF status gets reported as Idle.)
- When the H.323 phone is not connected to Cisco Unified Communications Manager for any reason, such as the Ethernet cable is unplugged from the phone, the BLF status gets reported as Idle all the time. (For presentities of phones that are running either SCCP or SIP and that are not connected to Cisco Unified Communications Manager, the BLF status gets reported as Unknown.)

**Configuring Presence**

This section contains information on the following topics:

- Configuring Presence Service Parameters and Enterprise Parameters, page 37-13
- Configuring and Applying the SUBSCRIBE Calling Search Space, page 37-14
- Finding Presence Groups, page 37-15
- Configuring Presence Groups, page 37-16
- Presence Group Configuration Settings, page 37-17
- Deleting a Presence Group, page 37-17
- Applying a Presence Group, page 37-18
- Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, page 37-20
- Configuring BLF/SpeedDial Buttons, page 37-20
- BLF/SpeedDial Configuration Settings, page 37-21

**Tip** Before you configure presence, review the “Configuration Checklist for Presence” section on page 37-1.

**Configuring Presence Service Parameters and Enterprise Parameters**

To configure presence enterprise parameters, for example, the BLF for Call List parameter, in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. For information on the parameter, click the question mark that displays in the Enterprise Parameter Configuration window or click the link for the parameter name.

To configure presence service parameters, for example, the Default Inter-Presence Group Subscription parameter, perform the following procedure:

**Tip** The Default Inter-Presence Group Subscription parameter does not apply to BLF/SpeedDials.
**Configuring Presence**

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose **System > Service Parameters**.

**Step 2** From the Server drop-down list box, choose the server where you want to configure the parameter.

**Step 3** From the Service drop-down list box, choose the Cisco CallManager (Active) service.

If the service does not display as active, ensure that the service is activated in Cisco Unified Serviceability.

**Step 4** Locate the clusterwide service parameters for the Presence feature.

**Tip** For information on the parameters, click the parameter name or click the question mark that displays in the Service Parameter Configuration window.

**Step 5** Update the parameter values.

**Step 6** Click **Save**.

**Additional Information**

See the “Related Topics” section on page 37-22.

**Configuring and Applying the SUBSCRIBE Calling Search Space**

All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box in the Trunk Configuration or Phone Configuration window.

The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes presence requests that come from the trunk or the phone. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space defaults to None.

To configure a calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces (Call Routing > Class of Control > Calling Search Space). For information on how to configure a calling search space, see the “Calling Search Space Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

To apply a SUBSCRIBE Calling Search Space to the SIP trunk, phone, or end user, perform the following procedure:

**Procedure**

**Step 1** Perform one of the following tasks:

- Find a phone, as described in the “Cisco Unified IP Phone Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

- Find a SIP trunk, as described in the “Trunk Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

- Find an end user, as described in the “End User Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.
Step 2  After the configuration window displays, choose the calling search space from the SUBSCRIBE Calling Search Space drop-down list box.

Step 3  Click Save.

Step 4  Click Reset.

Additional Information
See the “Related Topics” section on page 37-22.

Finding Presence Groups

The Find and List window for presence groups allows you to search for presence groups, which are used with the presence feature for authorization. To find a presence group, perform the following procedure:

Procedure

Step 1  Choose System > Presence Group.

The Find and List Presence Groups window displays. Records from an active (prior) query may also display in the window.

Step 2  To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records
- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note  To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3  Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Note  You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All and then clicking Delete Selected.

Step 4  From the list of records that display, click the link for the record that you want to view.
Configuring Presence Groups

To add, update, or copy presence groups, perform the following procedure:

Procedure

Step 1: In Cisco Unified Communications Manager Administration, choose System > Presence Group.

Step 2: Perform one of the following tasks:

- To add a new presence group, click the Add New button and continue with Step 3.
- To copy an existing presence group, locate the appropriate group as described in “Finding Presence Groups” section on page 37-15, click the Copy button or Copy icon next to the presence group that you want to copy, and continue with Step 3.
- To update an existing presence group, locate the appropriate group as described in “Finding Presence Groups” section on page 37-15 and continue with Step 3.
- To rename a presence group, locate the group as described in “Finding Presence Groups” section on page 37-15, click the Name link for group on the list, enter the new name when the window displays, and continue with Step 4.

Step 3: Enter the appropriate settings as described in Table 37-3.

Step 4: Click Save.

Additional Steps

After you configure the presence groups, apply the presence group configuration to the phone that is running either SIP or SCCP, SIP trunk, directory number, application user (for application users sending presence requests over the SIP trunk), or end user in Cisco Unified Communications Manager Administration. See the “Applying a Presence Group” section on page 37-18.

Additional Information

See the “Related Topics” section on page 37-22.
Presence Group Configuration Settings

Presence authorization works with presence groups. Table 37-3 describes the presence group configuration settings. Before you configure these settings, review the “Presence Group and Presence Authorization Tips” section on page 37-19. For related procedures, see the “Related Topics” section on page 37-22.

Table 37-3 Presence Group Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the presence group that you want to configure; for example, Executive_Group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the presence group that you are configuring.</td>
</tr>
<tr>
<td>Modify Relationship to Other Presence Groups</td>
<td>Select one or more presence groups to configure the permission settings for the named group to the selected group(s).</td>
</tr>
<tr>
<td>Subscription Permission</td>
<td>For the selected presence group(s), choose one of the following options from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td>• Use System Default—Set the permissions setting to the Default Inter-Presence Group Subscription clusterwide service parameter setting (Allow Subscription or Disallow Subscription).</td>
</tr>
<tr>
<td></td>
<td>• Allow Subscription—Allow members in the named group to view the real-time status of members in the selected group(s).</td>
</tr>
<tr>
<td></td>
<td>• Disallow Subscription—Block members in the named group from viewing the real-time status of members in the selected group(s).</td>
</tr>
</tbody>
</table>

The permissions that you configure display in the Presence Group relationship pane when you click Save. All groups that use system default permission setting do not display.

Deleting a Presence Group

This section describes how to delete a presence group from the Cisco Unified Communications Manager database.

Before You Begin

Before you can delete a presence group from Cisco Unified Communications Manager Administration, you must apply another group to the devices/user or delete all devices/users that use the presence group.

To find out which devices/users use the presence group, click the Name link for the presence group in the Find and List window; then, choose Dependency Records from the Related Links drop-down list box when the Presence Group Configuration window displays; click Go.

If the dependency records feature is not enabled for the system, enable dependency records in the System > Enterprise Parameters window. For more information about dependency records, see the Cisco Unified Communications Manager System Guide.

Procedure

1. Find the presence group by using the procedure in the “Finding Presence Groups” section on page 37-15.
Step 2  To delete multiple presence groups, check the check boxes next to the appropriate presence group in the Find and List window; then, click the Delete Selected icon or the Delete Selected button.

Step 3  To delete a single presence group, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate presence group; then, click the Delete Selected icon or the Delete Selected button.
- In the Find and List window, click the Name link for the presence group. After the specific Presence Group Configuration window displays, click the Delete icon or the Delete button.

Step 4  When prompted to confirm the delete operation, click OK to delete or Cancel to cancel the delete operation.

Additional Information
See the “Related Topics” section on page 37-22.

Applying a Presence Group

For information on configuring presence groups in Cisco Unified Communications Manager Administration, see the “Understanding Presence Groups” section on page 37-7. For information about configuring permission settings for presence authorization, see the “Understanding Presence Authorization” section on page 37-9. The system always allows presence requests between members in the same presence group.

To apply a presence group to the directory number, SIP trunk, phone that is running SIP, phone that is running SCCP, application user (for application users that are sending presence requests over the SIP trunk), or end user, perform the following procedure:

Procedure

Step 1  Perform one of the following tasks:

- Find a SIP trunk, as described in the “Trunk Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
- Find an application user, as described in the “Application User Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
- Find an end user, as described in the “End User Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
- Find a phone that is running either SCCP or SIP, as described in the “Cisco Unified IP Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

Tip  After the Phone Configuration window displays, you can access the Directory Number Configuration window by clicking the Line link in the Association Information pane. In the Directory Number Configuration window, you specify the presence group for the directory number.

When an administrator decides to add or change a BLF/SpeedDial button, the administrator ensures that the watcher is authorized to monitor that destination.
Step 2 After the configuration page displays, choose the group from the Presence Group drop-down list box. See the “Presence Group and Presence Authorization Tips” section on page 37-19 for provisioning tips.

Step 3 Click Save.

Step 4 For devices, you must click Reset.

Step 5 Repeat the procedure for all items that are listed in Step 1.

**Additional Information**

See the “Related Topics” section on page 37-22.

**Presence Group and Presence Authorization Tips**

Presence authorization works with presence groups. This section lists tips to use when you are configuring presence groups for presence authorization.

- To allow a watcher to monitor a destination, make sure that the presence group that is applied to the watcher that is originating the request, including application users, has permission to monitor the group that is applied to the presence entity. End users for supported applications, for example, Cisco Unified Communications Manager Assistant end users, also serve as watchers because the user requests status about a presence entity that is configured on the application.

- To allow Cisco Unified Communications Manager to receive and route presence requests from the SIP trunk application, make sure that the Accept Presence Subscription check box is checked in the Application User Configuration window to authorize incoming SUBSCRIBE requests. If no presence group is applied to the application user, Cisco Unified Communications Manager uses the presence group that is applied to the trunk.

- If you check the Accept Presence Subscription check box for an application user, but do not check the Accept Presence Subscription check box (in the SIP Trunk Security Profile Configuration window) that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.

- If you check the Accept Presence Subscription check box for an application user, but do not check the Enable Application Level Authorization check box (in the SIP Trunk Security Profile Configuration window) that is applied to the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.

- If digest authentication is not configured for the SIP trunk, you can configure the trunk to accept incoming subscriptions, but application-level authorization cannot be initiated, and Cisco Unified Communications Manager will accept all incoming requests before performing group authorization.

- If the SIP trunk uses digest authentication, as configured in the SIP Trunk Security Profile Configuration window, incoming presence requests require authentication of the credentials from the sending device. When digest authentication is used with application-level authorization, Cisco Unified Communications Manager also authenticates the credentials of the application that is sending the presence requests.

- After authorization and authentication is successful for a SIP trunk application, Cisco Unified Communications Manager performs group authorization to verify the group permissions that are associated with the SUBSCRIBE request before accepting the request.

- When an administrator decides to add or change a BLF/SpeedDial button for a SIP URI, the administrator ensures that the watcher is authorized to monitor that destination. If the system uses a SIP trunk to reach a SIP URI BLF target, the presence group associated with the SIP trunk applies.
When configuring a SIP URI as BLF/SpeedDial button, make sure the routing patterns are appropriately configured. See “SIP Route Pattern Configuration” in the Cisco Unified Communications Manager Administration Guide for more information.

Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons

Administrators can configure BLF/SpeedDial buttons for a phone, or user device profile. The Add a new BLF SD link does not display in the Association Information pane unless you configure a customized phone button template for BLF/SpeedDial buttons and apply the template to the phone or user device profile. After you apply the template to the phone or device profile (and save the phone or device profile configuration), the Add a new BLF SD link displays in the Association Information pane.

Tip
If the template does not support BLF/SpeedDials, the Add a new BLF SD link displays in the Unassigned Associated Items pane.

To configure a customized phone button template for BLF/SpeedDial buttons, perform the following procedure:

Procedure

1. Find the phone button template for the device, as described in the “Phone Button Template Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
2. After the Find/List window displays, click the Copy button or Copy icon for the phone button template.
3. In the Button Template Name field, enter a new name for the template; for example, BLF SIP 7970.
4. Click Save.
5. After the Phone Button Template Configuration window displays, choose Speed Dial BLF from the Feature drop-down list box(es); that is, if you want the line to be configured as a BLF/SpeedDial button.
6. Click Save.
7. If you are updating an existing customized phone button template that you already applied to phones, click Reset.

Configuring BLF/SpeedDial Buttons

To configure BLF/SpeedDial buttons, perform the following procedure:

Procedure

1. To configure the BLF/SpeedDial button in the Phone Configuration window, find a phone, as described in the “Cisco Unified IP Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
2. To configure the BLF/SpeedDial button for user device profiles, find the user device profile as described in the “Device Profile Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.
**Step 3**  After the configuration window displays, click the **Add a New BLF SD** link in the Association Information pane.

---

**Tip**  The link does not display in the Association Information pane if the phone button template that you applied to the phone or device profile does not support BLF/SpeedDials. The link displays in the Unassigned Associated Items pane if the phone button template does not support BLF/SpeedDials.

---

**Step 4**  Configure the settings, as described in Table 37-4. Administrators must ensure that the watcher is authorized to monitor a destination that is configured as a BLF/SpeedDial button.

**Step 5**  After you complete the configuration, click **Save** and close the window. The destination(s) and/or directory number(s) display in the pane.

---

**Additional Information**
See the “Related Topics” section on page 37-22.

---

### BLF/SpeedDial Configuration Settings

With the presence feature, a watcher can monitor the status of the presence entity (also called presentity). When you configure BLF/SpeedDial buttons, the presence entity displays as a speed dial on the device of the watcher.

Table 37-4 describes the settings that you configure for BLF/SpeedDial buttons. For more information on presence, see the “Related Topics” section on page 37-22.

**Table 37-4  BLF/SpeedDial Button Configuration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination | Perform one of the following tasks to configure a SIP URI or a directory number as a BLF/SpeedDial button:  
  • Only for phones that are running SIP, enter the SIP URI.  
    For phones that are running SCCP, you cannot configure SIP URI as BLF/SpeedDial buttons.  
  • For phones that are running either SCCP or SIP, enter a directory number in this field or go to the Directory Number drop-down list box.  
    If you want to configure non-Cisco Unified Communications Manager directory numbers as BLF/SpeedDial buttons, enter the directory number in this field.  
    For this field, enter only numerals, asterisks (*), and pound signs (#).  
    If you configure the Destination field, do not choose an option from the Directory Number drop-down list box.  
    If you choose an option from the Directory Number drop-down list box after you configure the Destination, Cisco Unified Communications Manager deletes the Destination configuration. |
Table 37-4  BLF/SpeedDial Button Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number</td>
<td>The Directory Number drop-down list box displays a list of directory numbers that exist in the Cisco Unified Communications Manager database. Configure this setting only if you did not configure the Destination field. For phones that are running either SCCP or SIP, choose the number (and corresponding partition, if it displays) that you want the system to dial when the user presses the speed-dial button; for example, 6002-Partition 3. Directory numbers that display without specific partitions belong to the default partition.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the text that you want to display for the BLF/SpeedDial button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that displays in the Label ASCII field.</td>
</tr>
<tr>
<td>Label ASCII</td>
<td>Enter the text that you want to display for the speed-dial button. The ASCII label represents the noninternationalized version of the text that you enter in the Label field. If the phone does not support internationalization, the system uses the text that displays in this field. <strong>Tip</strong>: If you enter text in the Label ASCII field that differs from the text in the Label field, Cisco Unified Communications Manager Administration accepts the configuration for both fields, even though the text differs.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuration Checklist for Presence, page 37-1
- Introducing Presence, page 37-4
- Understanding How Presence Works with Phones and Trunks, page 37-5
- Understanding How Presence Works with Route Lists, page 37-6
- Understanding Presence Groups, page 37-7
- Understanding Presence Authorization, page 37-9
- Understanding How the SUBSCRIBE Calling Search Space Works, page 37-11
- Presence Feature Interactions/Restrictions, page 37-12
- Configuring Presence Service Parameters and Enterprise Parameters, page 37-13
- Configuring and Applying the SUBSCRIBE Calling Search Space, page 37-14
- Finding Presence Groups, page 37-15
- Configuring Presence Groups, page 37-16
- Presence Group Configuration Settings, page 37-17
- Deleting a Presence Group, page 37-17
- Applying a Presence Group, page 37-18
• Configuring a Customized Phone Button Template for BLF/SpeedDial Buttons, page 37-20
• Configuring BLF/SpeedDial Buttons, page 37-20
• BLF/SpeedDial Configuration Settings, page 37-21

Additional Documentation
• Digest Authentication, *Cisco Unified Communications Manager Security Guide*
• Authorization, *Cisco Unified Communications Manager Security Guide*
• Phone administration documentation that supports your phone and this version of Cisco Unified Communications Manager
• User documentation for Cisco Unified IP Phone or phone that is running SIP
• Firmware release notes for your phone
Quality Report Tool

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, acts as a service that allows users to easily and accurately report audio and other general problems with their IP phone. QRT automatically loads with the Cisco Unified Communications Manager installation, and the Cisco Extended Functions (CEF) service supports it. (For more information about the Cisco Extended Functions service, see the *Cisco Unified Serviceability Administration Guide*.)

As system administrator, you can enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from two different user modes, depending upon the amount of user interaction with QRT that is desired.

**Note**
The system gives users with administrator privileges the authorization to configure QRT and view the reports.

This chapter provides the following information about configuring and using the QRT feature:

- Configuration Checklist for QRT, page 38-2
- Introducing Quality Report Tool, page 38-3
- System Requirements for QRT, page 38-6
- Cisco Extended Functions Service Dependency, page 38-7
- Securing a TLS Connection to CTI, page 38-8
- How to Use QRT, page 38-9
- Interactions and Restrictions, page 38-15
- Installing and Activating QRT Functions, page 38-15
- Configuring the QRT Feature, page 38-16
- Using the QRT Viewer, page 38-25
- Providing Information to Users for the QRT Feature, page 38-30
- Troubleshooting the QRT Feature, page 38-30
- Related Topics, page 38-32
The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, acts as a service that allows users to easily and accurately report audio and other general problems with their IP phone. QRT automatically loads with the Cisco Unified Communications Manager installation, and the Cisco Extended Functions (CEF) service supports it. (For more information about the Cisco Extended Functions service, see the Cisco Unified Serviceability Administration Guide.)

As system administrator, you can enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from different user modes, depending upon the amount of user interaction with QRT that is desired.

Table 38-1 shows the steps for configuring the QRT feature in Cisco Unified Communications Manager. For additional information, see the “Related Topics” section on page 38-32.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Create a copy of the Standard User softkey template and add the QRT softkey for the following call states:</td>
</tr>
<tr>
<td>• On Hook</td>
<td>Creating a Softkey Template with the QRT Softkey, page 38-17</td>
</tr>
<tr>
<td>• Connected</td>
<td>Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
</tbody>
</table>

| **Step 2** | Add the new softkey template to the common device configuration. |
| **Step 3** | Add the new softkey template to the user phones by using the Phone Configuration window. |
| **Note** | You can assign the common device configuration to the phone configuration if you are using common device configuration for the softkey. Alternatively, you can add the softkey individually to each phone. |
| **Step 4** | Using the Cisco Unified Serviceability tool, Service Activation, activate Cisco Extended Functions service. |
| **Step 5** | From Cisco Unified Serviceability, configure alarms and traces for QRT. |
| **Step 6** | Configure the Cisco Extended Functions service parameters for QRT. |
| **Step 7** | Access the QRT Viewer to create, customize, and view IP phone problem reports. |

For additional information, see the “Related Topics” section on page 38-32.
Introducing Quality Report Tool

When you install Cisco Unified Communications Manager, the Cisco Extended Functions service installs and loads the QRT functionality on the Cisco Unified Communications Manager server.

Then, as system administrator, you enable the QRT feature through the use of softkey templates and define how the feature will work in your system by configuring system parameters and setting up Cisco Unified Serviceability tools. You can then create, customize, and view phone problem reports by using the QRT Viewer application. (The system includes the QRT Viewer application as part of the Real Time Monitoring Tool. See the “Using the QRT Viewer” section on page 38-25 for more information.)

You can configure QRT availability for up to four different call states and choose from two different user modes. The user modes determine the level of user interaction that is enabled with QRT and allow either detailed voice-quality reports or more general phone problem reports and relevant statistics. (See the “Extended Menu Choices” section on page 38-10 for more information.)

When users experience problems with their IP phones, they can invoke this feature by pressing the QRT softkey on their Cisco Unified IP Phone during the Connected call state.

From a supported call state, and using the appropriate problem classification category, users can then choose the reason code that best describes the problem that they are experiencing with their IP phone. See the “Problem Classification Categories and Reason Codes” section on page 38-11 for specific information about problem categories, reason codes, and supported call states.

The Quality Report Tool comprises several key components. The following sections provide information about these components and the architecture of the QRT feature:

- Components of QRT, page 38-3
- Overview of QRT Architecture, page 38-4

Additional Information

See the “Related Topics” section on page 38-32.

Components of QRT

QRT, a multitiered, web-based application, includes the following key components:

- Client Components
  - IP phone browser for end-user interface
  - Cisco Unified Communications Manager Administration windows for feature and tools configuration and viewer application
- Server Components
  - Cisco Extended Functions service
  - Cisco Unified Communications Manager for skinny messages
  - CTIManager for QBE messages
  - Database for configuration data and device data
  - Cisco RIS Data Collector for runtime device-related information
  - Alarm interface
  - System Diagnostic Interface (SDI) trace
Introducing Quality Report Tool

- Service—Cisco Extended Functions service for collecting and managing user reports. It also handles the user interface on the IP phone as well as notifying Cisco RIS Data Collector for alerts and issuing SNMP traps.
- Viewer Application—The QRT Viewer application, which is included as part of the trace collection feature in the Cisco Real Time Monitoring Tool (RTMT), allows you to filter, format, and view generated reports. Reports automatically open in the QRT Viewer when you view a trace file that includes QRT information.

Additional Information
See the “Related Topics” section on page 38-32.

Overview of QRT Architecture

The QRT feature uses the Cisco Extended Functions service, which comprises the following interfaces:

- Cisco CTIManager Interface (QBEHelper), page 38-5
- Cisco Unified Communications Manager Database Interface (DBL Library), page 38-5
- Screen Helper and Dictionary, page 38-5
- Redundancy Manager, page 38-6
- DB Change Notifier, page 38-6
- SDI Trace and Alarm, page 38-6

The Cisco Extended Functions service interfaces with the phone by using the XML services interface (XSI) over skinny protocol (a protocol that is used between a Cisco Unified IP Phone and Cisco Unified Communications Manager) and the Quick Byte Encoding protocol (a protocol that is used between the Cisco CTIManager and TSP/JTAPI).

When a user presses the QRT softkey, QRT opens the device and presents up to four different screens that display problem categories and associated reason codes to obtain user feedback.

After the user chooses the option that best describes the problem, the system logs the feedback in the XML file; the system then issues alarms to notify the Cisco RIS Data Collector to generate alerts and SNMP traps. When QRT detects that user interaction is complete, it then closes the device.

Note
The actual information that is logged depends upon the user selection and whether the destination device is a Cisco Unified IP Phone.
Figure 38-1 shows an illustration of the Cisco Extended Functions service architecture.

**Cisco CTI Manager Interface (QBEHelper)**

The QBEHelper library provides the interface that allows the Cisco Extended Functions service to communicate with a configured Cisco CTI Manager.

**Cisco Unified Communications Manager Database Interface (DBL Library)**

The DBL library provides the interface that allows the Cisco Extended Functions service to perform queries on various devices that are configured and registered in the Cisco Unified Communications Manager database.

**Screen Helper and Dictionary**

The screen helper of the Cisco Extended Functions service reads the XML dictionary files and creates Document Object Model (DOM) objects for all installed locales when the CEF service starts. The system uses these DOM objects for constructing XSI screens that the Cisco Unified IP Phone needs.
Redundancy Manager

When multiple Cisco Extended Functions are active within a Cisco Unified Communications Manager cluster, the redundancy manager uses an algorithm to determine which CEF service is active and which is the backup CEF. The Redundancy Manager uses the lowest IP address of the server that is running the CEF service as the active service. The remaining CEF services serve as backup services.

DB Change Notifier

The DB Change Notifier handles all the database change notifications, such as service parameter changes, trace parameter changes, alarm configuration changes, and status changes of other Cisco Extended Functions services in the cluster, and reports the changes to the CEF service.

SDI Trace and Alarm

The Cisco Extended Functions service uses the SDI Trace and Alarm libraries. The libraries generate traces and alarms to the Event Viewer. The alarm library publishes information about the CEF service to Syslog, SNMP, and the Cisco RIS Data Collector service. For more information about traces and alarms, see the Cisco Unified Serviceability Administration Guide.

Additional Information

See the “Related Topics” section on page 38-32.

System Requirements for QRT

To operate, the QRT feature requires the following software components:

- Cisco Unified Communications Manager
- Cisco Real-Time Monitoring Tool

Support for the QRT feature extends to any model IP phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- An internal HTTP server

Note

For more information, see the following URL for the appropriate Cisco Unified IP Phone guide for your model IP phone:

Additional Information

See the “Related Topics” section on page 38-32.
Cisco Extended Functions Service Dependency

The Cisco Extended Functions service depends on the following services:

- Cisco CallManager—Ensure a minimum of one Cisco CallManager service is running in the cluster, but the service need not be on the same server as CEF.
- Cisco CTIManager—Ensure a minimum of one Cisco CTIManager service is running in the cluster, but the service need not be on the same server as CEF.
- Cisco Database Layer Monitor—Ensure one Cisco Database Layer Monitor service is running on the same server as CEF.
- Cisco RIS Data Collector—Ensure one Cisco RIS Data Collector service is running on the same server as CEF.

**Note**

Ensure Cisco Database Layer Monitor and Cisco RIS Data Collector are running on the same server. You can include more than one CEF service in a Cisco Unified Communications Manager cluster.

**Tip**

Install all the services on one server for one-server Cisco Unified Communications Manager systems.

*Figure 38-2* shows a typical Cisco Extended Functions service configuration.

**Figure 38-2  Cisco Extended Functions Service Dependency (Typical Configuration)**

Additional Information

See the “Related Topics” section on page 38-32.
Multiple Cisco Extended Functions Applications in a Cluster

If multiple Cisco Extended Functions services are active within a Cisco Unified Communications Manager cluster, CEF uses an algorithm to determine which service should be active and to order the remaining as backups. The CEF application with the lowest IP address becomes active. The service with the next lowest IP address becomes the backup to the active service. Any remaining services act as backups to each other, beginning with the service with the next lowest IP address. If you add any new services to the cluster, CEF restarts the algorithm to determine which service will be active.

Note
When a Cisco Extended Functions service gets started in a cluster, the CEF service with the lowest IP address becomes active. This process may cause service interruption for approximately 2 minutes.

To verify the directory status and Cisco Extended Functions service registration status to the Cisco CTI Manager, use the Real Time Monitoring Tool as described in the Cisco Unified Real Time Monitoring Tool Administration Guide.

Additional Information
See the “Related Topics” section on page 38-32.

Securing a TLS Connection to CTI

QRT supports a secure Transport Layer Security (TLS) connection to CTI. Obtain the secure connection by using the “CCMQRTSecureSysUser” application user, as described in the following procedure.

Note
If you enable security from the Service Parameter Configuration window, the QRT will open a secure connection to CTI Manager by using the Application CAPF profile. You should configure both the “CTI Manager Connection Security Flag” and the “CAPF Profile Instance Id for Secure Connection to CTI Manager” service parameters for the secure connection to succeed. See the “Setting the Cisco Extended Functions Service Parameters for QRT” section on page 38-24. For more information, see “Application User CAPF Profile Configuration” and “Service Parameter Configuration” in the Cisco Unified Communications Manager Administration Guide.

Note
You must also configure the security service parameter “Cluster Security Mode CAPF Phone Port” to secure a TLS connection to CTI, giving it a value of 1. You can do this from System > Enterprise Parameters in Cisco Unified Communications Manager Administration. See “Enterprise Parameter Configuration” in the Cisco Unified Communications Manager Administration Guide.

Perform the following procedure to configure the application user.

Procedure

Step 1
From Cisco Unified Communications Manager Administration, choose User Management > Application User.

The Find and List Application Users window displays.

Step 2
Click Find.
Step 3  From the Find and List Application Users Configuration window, click `CCMQRTSecureSysUser` or `CCMQRTSysUser`.

Note  To configure a CAPF profile, see “Application User CAPF Profile Configuration” in the *Cisco Unified Communications Manager Administration Guide* for general information and to the *Cisco Unified Communications Manager Security Guide* for details.

Additional Information  See the “Related Topics” section on page 38-32.

**How to Use QRT**

After you properly install and configure QRT, the QRT softkey can be configured on certain Cisco Unified IP Phone models. See the “System Requirements for QRT” section on page 38-6 for the IP phone models that are supported with QRT.

Note  The Cisco Unified Communications Manager Standard User template does not include the QRT softkey. You must enable QRT functionality and make it available to users through the use of a QRT softkey. To do this, create, configure, and assign the QRT softkey from Cisco Unified Communications Manager Administration. See the “Configuring the QRT Feature” section on page 38-16 for information about setting up the softkey template.

The following sections describe the user interaction features with QRT:

- **User Interface**, page 38-9
- **Extended Menu Choices**, page 38-10
- **Problem Classification Categories and Reason Codes**, page 38-11

For more user-related information, see the following URL for the appropriate Cisco Unified IP Phone guide for your phone model:


Additional Information  See the “Related Topics” section on page 38-32.

**User Interface**

The QRT user interface includes several components:

- **Phone Screens**—Available to all IP phones that are in the common device configuration where the QRT softkey is configured, the phone screen supports different locales.

Only the Cisco Unified Communications Manager administrator can access the following components:

- **Serviceability**—See the “Configuring the Cisco Unified Serviceability Features” section on page 38-21.
How to Use QRT

- Alert Configuration—See the “Configuring Alarms and Traces for QRT” section on page 38-22.
- Service Parameters—See the “Setting the Cisco Extended Functions Service Parameters for QRT” section on page 38-24.
- Viewer Application—See the “Using the QRT Viewer” section on page 38-25.

Figure 38-3 shows an example of the QRT softkey as it displays on a Cisco Unified IP Phone.

Additional Information
See the “Related Topics” section on page 38-32.

Extended Menu Choices

Extended menu choices allow a user to interact with QRT and provide additional details regarding the phone problem that they are reporting. You can choose to enable extended menu choices or provide users with a more passive interface, depending upon the amount of information that you want users to submit.

From the Cisco Unified Communications Manager Service Parameters Configuration window, configure the user interface mode for QRT from the following options:

- Silent Mode—In this mode, the user does not get presented with extended menu choices. When the user presses the QRT softkey, the system collects the streaming statistics and logs the report without additional user interaction.

The system supports silent mode only when the IP phone is in the Connected call state.

Figure 38-4 shows an example of the QRT display as it appears in silent mode.
Interview Mode—In this mode, the user gets presented with extended menu choices, which allow additional user input that is related to audio quality on the IP phone (see the “Problem Classification Categories and Reason Codes” section on page 38-11 for the applicable reason codes). This mode also allows the user to report other, non-audio-related problems such as the phone rebooting or the inability to make calls.

The system supports interview mode only when the IP phone is in the Connected or On Hook call state.

Figure 38-5 shows an example of the QRT display as it appears when the QRT softkey is pressed while the phone is on hook and in interview mode.

**Figure 38-5  QRT Phone Interface - On Hook, Interview Mode Display**

<table>
<thead>
<tr>
<th>Select Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems with last call</td>
</tr>
<tr>
<td>Phone recently rebooted</td>
</tr>
<tr>
<td>Can’t make calls</td>
</tr>
</tbody>
</table>

**Note**
Ensure that you configure the QRT softkey only for the supported call states.

**Note**
Configure the “Display Extended QRT Menu Choices” field in the Cisco Unified Communications Manager Administration Service Parameters configuration window to determine whether the users can access the extended menu choices. See the “Setting the Cisco Extended Functions Service Parameters for QRT” section on page 38-24 for additional information.

**Additional Information**
See the “Related Topics” section on page 38-32.

**Problem Classification Categories and Reason Codes**

The following tables show the problem categories and corresponding reason codes that users can choose when they report problems with their IP phones:

- Additional options become available after you configure extended menu choices.
- Users can choose only one reason code per category, per problem.
- Each problem category becomes available only when the IP phone is in the supported call state.
Table 38-2 shows the supported call states and the reason codes that are available for the “Problems with current call” category.

### Table 38-2  Problem Category—Problems with Current Call

<table>
<thead>
<tr>
<th>Problem Category</th>
<th>Supported Call States</th>
<th>Reason Codes</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems with current call</td>
<td>• Connected</td>
<td>• I hear echo</td>
<td>The system collects streaming statistics from the source and destination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The remote end hears echo</td>
<td>devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Choppy audio</td>
<td>Note：Source device/IP phone refers to the device on which the QRT softkey</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Robotic sound</td>
<td>gets pressed. For example, “source” and “destination” in this case do not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Long delays</td>
<td>see the calling party and called party in a connected call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low volume</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The remote end experiences low volume</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I can’t hear the remote end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The remote end can’t hear me</td>
<td></td>
</tr>
</tbody>
</table>

Figure 38-6 shows an example of the phone display as it appears after the QRT softkey is pressed on an IP phone in the connected state. This menu allows the user to provide additional details before submitting a problem with the current phone call.

![Figure 38-6 Reporting Problem with the Current Call](image)
Table 38-3 shows the supported call state and the reason codes that are available for the “Problems with last call” category.

**Table 38-3  Problem Category—Problems with Last Call**

<table>
<thead>
<tr>
<th>Problem Category</th>
<th>Supported Call States</th>
<th>Reason Codes</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems with last call</td>
<td>• On Hook</td>
<td>• I heard echo</td>
<td>The system collects streaming statistics from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The remote end heard echo</td>
<td>source device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Choppy audio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Robotic sound</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Long delays</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low volume on my end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low volume on the remote end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I could not hear the remote end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The remote end could not hear me</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The call dropped</td>
<td></td>
</tr>
</tbody>
</table>

Figure 38-7 shows an example of the phone display as it appears after the user selects the “Problems with last call” category. This menu allows the user to provide additional details before submitting a problem report for the last phone call.

**Figure 38-7  Reporting Problem with the Last Call**

![Image of phone display]

Table 38-4 shows the supported call state that is available for the “Phone recently rebooted” category. No associated reason codes exist for this category.

**Table 38-4  Problem Category—Phone Recently Rebooted**

<table>
<thead>
<tr>
<th>Problem Category</th>
<th>Supported Call States</th>
<th>Reason Codes</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone recently rebooted</td>
<td>• On Hook</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Figure 38-8 shows an example of the phone display after the user chooses the “Phone recently rebooted” category. The system logs user feedback.

Figure 38-8 Reporting Problem with Phone That Recently Rebooted

Table 38-5 shows the supported call state and the reason codes that are available for the “I can’t make calls” category.

Table 38-5 Problem Category—I Can’t Make Calls

<table>
<thead>
<tr>
<th>Problem Category</th>
<th>Supported Call States</th>
<th>Reason Codes</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>I can’t make calls</td>
<td>• On Hook</td>
<td>• I get a busy tone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I get a fast busy tone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I get dial tone after dialing digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I hear silence after dialing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I don’t get dial tone</td>
<td></td>
</tr>
</tbody>
</table>

Figure 38-9 shows an example of the phone display as it appears after the user chooses the “I can’t make calls” category.

Figure 38-9 Reporting Problem with I Can’t Make Calls

Note QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, the Cisco Unified Communications Manager database, and the user. “Source” and “destination” in this case do not see the calling party and called party in a connected call. See the “QRT Reports” section on page 38-26 for detailed information about the fields that the phone problem report includes.
Interactions and Restrictions

The following interactions and restrictions apply when you use the QRT feature with Cisco Unified Communications Manager:

- Ensure that Cisco Extended Functions, Cisco CallManager, CTI Manager, and Cisco RIS Data Collector services are running and fully operational.
- As system administrator, you must create, configure, and assign softkey templates to enable the QRT softkey feature on IP phones.
- Ensure that you configure the QRT softkey only for the supported call states.
- The system makes the extended menu choices option available only when the “Display Extended QRT Menu Choices” service parameter is set to True; it provides support for the “Problems with current call” category.
- If another application feature (such as Cisco Call Back or Cisco Unified Communications Manager Assistant) or a function key (such as Settings, Directories, or Messages) is invoked while the user is interacting with QRT, or if the user does not complete the QRT selection, the system can overwrite the QRT display. In this case, the system forces the device into a wait state, which prevents QRT from completing the interaction and then closes the device.

Note: Because unattended devices consume large amounts of resources and could impact CTI performance, the system configures QRT to regularly check for opened devices. You cannot modify these system settings.

- Phone that is running SIP that is configured to use UDP as the transport, instead of TCP, will not support the “device data pass-through” functionality. QRT requires the pass-through functionality, so QRT does not support these UDP-configured phones that are running SIP.
- The Quality Report Tool supports IPv6 if the device uses an IP Addressing Mode of IPv4 Only or IPv4 and IPv6 (dual-stack mode). Users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only. For more information on IPv6, see the “Internet Protocol Version 6 (IPv6)” section on page 29-1.

Installing and Activating QRT Functions

As a feature within the Cisco Extended Functions service, QRT automatically installs as part of the Cisco Unified Communications Manager installation.
Perform the following steps after installation to enable QRT availability for users and to set up administrative reporting capabilities:

1. Properly configure the QRT feature for Cisco Unified IP Phone users. See the “Configuring the QRT Feature” section on page 38-16.

2. From Cisco Unified Serviceability, activate the Cisco Extended Functions service and configure alarms and traces for use with QRT. See the “Configuring the Cisco Unified Serviceability Features” section on page 38-21 and see the Cisco Unified Serviceability Administration Guide for additional information.

3. Define how the QRT feature will work in your system by configuring the applicable service parameters for the Cisco Extended Functions service. See the “Setting the Cisco Extended Functions Service Parameters for QRT” section on page 38-24.

4. Create, customize, and view phone problem reports by using the QRT Viewer application. See the “Using the QRT Viewer” section on page 38-25.

---

**Note**

If users require the QRT feature to display (softkeys and messages on the IP phone) in any language other than English, verify that the locale installer is installed before configuring QRT. See the Cisco Unified Communications Operating System Administration Guide for more information.

**Additional Information**

See the “Related Topics” section on page 38-32.

---

**Configuring the QRT Feature**

For successful configuration of the QRT feature, review the steps in Table 38-1, QRT Configuration Checklist, perform the configuration requirements, activate the Cisco Extended Functions service, and set the service parameters.

The following sections provide configuration information for enabling QRT:

- Creating a Softkey Template with the QRT Softkey, page 38-17
- Configuring the QRT Softkey Template in Common Device Configuration, page 38-19
- Adding the QRT Softkey Template in Phone Configuration, page 38-20
- Activating the Cisco Extended Functions Service for QRT, page 38-22
- Configuring Alarms and Traces for QRT, page 38-22
- Setting the Cisco Extended Functions Service Parameters for QRT, page 38-24
- Related Topics, page 38-32

**Tip**

Before you configure the QRT feature, review the “Configuration Checklist for QRT” section on page 38-2.
Creating a Softkey Template with the QRT Softkey

Perform the following procedure to create a new softkey template with the QRT softkey.

Procedure

**Step 1**
From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Softkey Template**.

**Step 2**
Click **Add New**. (Alternatively, you can click the **Find** button to view a list of the available softkey templates.)

- If you click the **Add New** button, choose the Standard User softkey template from the Create a softkey template based on drop-down list.
- If you click the **Find** button to view a list of the available softkey templates, choose the Standard User softkey template from the Softkey Template list.

**Step 3**
Click the **Copy** button.
The Softkey Template Configuration window displays with new information.

**Step 4**
In the Softkey Template Name field, enter a new name for the template; for example, QRT Standard User; then, add a description.

Figure 38-10 shows an example of the Cisco Unified Communications Manager Administration Softkey Template Configuration window where you copy a softkey template.

Figure 38-10  Softkey Template Configuration Window
Step 5  Click **Save**.

The Softkey Template Configuration redisplays with new information.

Step 6  To add an application, click the **Add Application** button. See the “Adding Application Softkeys to Nonstandard Softkey Templates” section of the *Cisco Unified Communications Manager Administration Guide* for detailed instructions.

Step 7  To add the QRT softkey to the template, choose **Configure Softkey Layout** from the Related Links drop-down list box on the Softkey Template Configuration window and click **Go**.

The Softkey Layout Configuration window displays.

**Note**  You must add the QRT softkey to the Connected and On Hook call states.

Step 8  To add the QRT softkey to the On Hook call state, choose **On Hook** from the call states drop-down list box.

The Softkey Layout Configuration window redisplays with the Unselected Softkeys and Selected Softkeys lists.

Step 9  From the Unselected Softkeys list, choose the **Quality Report Tool (QRT)** softkey and click the right arrow to move the softkey to the Selected Softkeys list.

You can prioritize the items in the Selected Softkeys list by using the up and down arrow keys.

**Figure 38-12** shows an example of the Cisco Unified Communications Manager Administration Softkey Layout Configuration window.
Step 10 To save and continue, click **Save**.

Step 11 To add the QRT softkey to the Connected call state, repeat **Step 8 through Step 10** for each individual call state.

**Note** Ensure that you configure the QRT softkey only for the supported call states and click the **Save** button after each entry.

**Additional Information**

See the “**Related Topics**” section on page 38-32.

**Configuring the QRT Softkey Template in Common Device Configuration**

Perform the following procedure to add the QRT softkey template to the common device configuration.

**Procedure**

**Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Common Device Configuration**.

**Step 2** Click **Find**.

**Step 3** Choose any previously created common device configuration that displays.

You can add the template to any customized common device configuration for QRT feature users.
Step 4  In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the “Creating a Softkey Template with the QRT Softkey” section on page 38-17.)

Note All IP phones that are part of this common device configuration inherit this softkey template to provide an easy way for you to assign softkey templates to multiple phones. To associate softkey templates to individual IP phones, see the “Adding the QRT Softkey Template in Phone Configuration” section on page 38-20.

Step 5  Click Save.

Additional Information
See the “Related Topics” section on page 38-32.

Adding the QRT Softkey Template in Phone Configuration

Perform the following procedure to add the QRT softkey template to each user phone.

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Device > Phone.

The Find and List Phones window displays.

Step 2  Find the phone to which you want to add the softkey template. See the “Phone Configuration Settings” section of the “Cisco Unified IP Phone Configuration” chapter in the Cisco Unified Communications Manager Administration Guide.

Step 3  In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box. (If you have not created this template, see the “Creating a Softkey Template with the QRT Softkey” section on page 38-17.)

If you alternatively configured the softkey template in the common device configuration, from the Common Device Configuration field, choose the common device configuration that contains the new softkey template.
Figure 38-13 shows an example of the Cisco Unified Communications Manager Administration Phone Configuration window.

**Figure 38-13   Phone Configuration**

![Phone Configuration Window](Image)

**Step 4** Click **Save**.

**Additional Information**

See the “Related Topics” section on page 38-32.

**Configuring the Cisco Unified Serviceability Features**

The Cisco Extended Functions service uses the following Cisco Unified Serviceability features:

- **Service Activation**—Configured from the Cisco Unified Serviceability Tools window.
- **SDI Trace**—Configured from the Cisco Unified Serviceability Trace Configuration window.
- **Alarm Interface**—Configured from the Cisco Unified Serviceability Alarm Configuration window.
- **Real Time Monitoring Tool (RTMT)**—Used to monitor the operating status of QRT and CTIManager. For detailed information about RTMT, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

This section describes how to activate and configure the Cisco Unified Serviceability features for use with QRT and contains the following information:

- Activating the Cisco Extended Functions Service for QRT, page 38-22
- Configuring Alarms and Traces for QRT, page 38-22
For additional information about Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide*.

### Activating the Cisco Extended Functions Service for QRT

Follow this procedure to activate the Cisco Extended Functions service for use with the QRT feature.

**Procedure**

**Step 1**
From the Navigation drop-down list box in Cisco Unified Communications Manager Administration, located in the upper, right corner of the window, choose Cisco Unified Serviceability and click **Go**.

The Cisco Unified Serviceability window displays.

**Step 2**
To activate the Cisco Extended Functions service, choose **Tools > Service Activation**.

A Server drop-down list box displays.

**Step 3**
From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to activate the Cisco Extended Functions service.

**Step 4**
Check the **Cisco Extended Functions** check box.

**Step 5**
Click **Save**.

The CEF activation status changes from deactivated to activated.

**Tip**
You can check the activation status of the Cisco Extended Functions service from Cisco Unified Serviceability by choosing **Tools > Control Center - Feature Services**. Look for Cisco Extended Functions; if the Cisco Extended Functions service is active, it displays as Activated.

### Configuring Alarms and Traces for QRT

Follow these procedures to configure alarms and SDI traces through Cisco Unified Serviceability.

**Procedure—Alarm Configuration**

**Step 1**
From the Cisco Unified Serviceability window, choose **Alarm > Configuration**.

A Server drop-down list box displays.

**Step 2**
From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure alarms.

**Step 3**
From the Service Group drop-down list box, choose CM Services.

**Step 4**
From the Service drop-down list box, choose **Cisco Extended Functions**.

**Step 5**
Check the **Enable Alarm** check box for both Local Syslogs and SDI Trace.
Step 6  From the drop-down list box, configure the Alarm Event Level for both Local Syslogs and SDI Trace by choosing one of the following options:
   - Emergency
   - Alert
   - Critical
   - Error
   - Warning
   - Notice
   - Informational
   - Debug
The default value specifies Error.

Step 7  Click Save.

---

**Procedure—Trace Configuration**

**Step 1** From the Cisco Unified Serviceability window, choose Trace > Configuration.
A Server drop-down list box displays.

**Step 2** From the Server drop-down list box, choose the Cisco Unified Communications Manager server on which you want to configure traces.

**Step 3** From the Service Group drop-down list box, choose CM Services.

**Step 4** From the Service drop-down list box, choose Cisco Extended Functions.

**Step 5** Check the following check boxes:
   - Trace On
   - Cisco Extended Functions Trace Fields

**Step 6** From the drop-down list box, configure the Debug Trace Level by choosing one of the following options:
   - Error
   - Special
   - State Transition
   - Significant
   - Entry_exit
   - Arbitrary
   - Detailed
The default value specifies Error.

**Note**  Cisco recommends that you check all the check boxes in this section for troubleshooting purposes.
Chapter 38      Quality Report Tool

Step 7   Click **Save**.

For additional information about configuring alarms and traces, see the *Cisco Unified Serviceability Administration Guide*.

### Setting the Cisco Extended Functions Service Parameters for QRT

Follow this procedure to set the Cisco Extended Functions service parameters by using Cisco Unified Communications Manager Administration.

**Note**

Cisco recommends that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs otherwise.

**Procedure**

1. **Step 1** If your display shows the Cisco Unified Serviceability window, from the Navigation drop-down list box, located in the upper, right corner of the window, choose Cisco Unified CM Administration and click **Go**.
2. **Step 2** The Cisco Unified CM Administration window displays. Choose **System > Service Parameters**.
3. **Step 3** A Server drop-down list box displays. Choose the Cisco Unified Communications Manager server where the QRT application resides.
4. **Step 4** A Service drop-down list box displays. Choose the Cisco Extended Functions service.
5. **Step 5** Configure the following Cisco Extended Functions service parameters for QRT.

   a. **Display Extended QRT Menu Choices**—Determines whether extended menu choices are presented to the user. You can choose one of the following configuration options:
      - Set this field to true to display extended menu choices (interview mode).
      - Set this field to false to not display extended menu choices (silent mode).
      - The recommended default value specifies false (silent mode).
   b. **Streaming Statistics Polling Duration**—Determines the duration that is to be used for polling streaming statistics. You can choose one of the following configuration options:
      - Set this field to -1 to poll until the call ends.
      - Set this field to 0 to not poll at all.
      - Set it to any positive value to poll for that many seconds. Polling stops when the call ends.
      - The recommended default value specifies -1 (poll until the call ends).
   c. **Streaming Statistics Polling Frequency (seconds)**—Designates the number of seconds to wait between each poll:
      - The value ranges between 30 and 3600.
      - The recommended default value specifies 30.
   d. **Maximum No. of Files**—Specifies the maximum number of files before the file count restarts and overwrites the old files:
      - The value ranges between 1 and 10000.
Using the QRT Viewer

You can use the QRT Viewer to view the IP phone problem reports that the Quality Report Tool generates. The QRT Viewer allows you to filter, format, and view the tool-generated phone problem reports, so they provide you with the specific information that you need.

- To view the QRT Viewer application, you need to install the Cisco Real Time Monitoring Tool (RTMT) plug-in, which includes the trace collection feature.
- The trace collection feature enables collection and viewing of log files; the QRT Viewer is included with the trace collection feature.

Note

For detailed information about installing and configuring the RTMT and trace collection feature, and for detailed information about accessing, configuring, using, and customizing the QRT Viewer for IP phone problem reports, see theCisco Unified Serviceability Administration Guide and theCisco Unified Real Time Monitoring Tool Administration Guide.
QRT Reports

QRT collects information from various sources, such as the source IP phone, the destination IP phone, the Cisco RIS Data Collector, Cisco Unified Communications Manager, and the user. (The system does not collect information from gateways or other devices.) “Source” and “destination” in this case, do not see the calling party and called party in a connected call.

Note
See the QRT Viewer chapter in the Cisco Unified Serviceability Administration Guide for additional information about QRT reports.

The following list provides information, segmented by information source, about the QRT report fields.

Information Collected from the Source Device

- Directory number of source device (in the case of multiline devices, the information shows only the first primary directory number)
- Source device type (for example, CP-7960, CP-7940)
- Source stream1 port number
- Source codec (for example, G.711u)
- Source packets (for example, 2,45,78)
- Source rcvr packets (for example, 12,45,78)
- Source rcvr jitter (for example, 0 0)
- Source rcvr packet lost (for example, 0,21 0,21)
- Source sampling timestamp, implicit (for example, 12:30, 13:00, 13:30, 14:00)
- Destination device name (IP)
- Destination stream1 port number

Note
The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data. Also, for the “Problems with last call” category, these values might reflect only the last snapshot of the streaming statistics that are stored in the phone device.

Information Collected from the Destination Device

The system collects the following information if the destination device is a supported Cisco Unified IP Phone within same Cisco Unified Communications Manager cluster. If the destination device is not an IP phone, the information includes only IP address, device name, and device type.

- Directory number of destination device (in the case of multiline devices, the information shows only the first primary directory number)
- Destination device type (for example, CP-7960, CP-7940)
• Destination codec
• Destination packets
• Destination rcvr packets
• Destination rcvr jitter
• Destination rcvr packet lost
• Destination sampling timestamp (Implicit)

Note
The number of samples that are collected for packets, jitter, packets lost, and so on, depends on the sampling duration and polling frequency. The streaming information gets collected only one time per call. For example, if phone A called phone B and both phone A and phone B submit multiple reports for the same call, only the first report includes the streaming data that is included. QRT attempts to collect the information from the destination IP phone only for the “Problems with current call” category.

Information Collected from RIS Data Collector
• Source device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)
• IP address for source device
• Registered Cisco Unified Communications Manager name for source device
• Source device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
• Source device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
• Source device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
• Destination device name
• Destination device type (if the device is not one of the supported IP phones; for example, RISCLASS_PHONE, RISCLASS_GATEWAY, RISCLASS_H323, RISCLASS_CTI, RISCLASS_VOICEMAIL)
• Destination device model (for example, DBLTypeModel::MODEL_TELECASTER_MGR, DBLTypeModel::MODEL_TELECASTER_BUSINESS)
• Destination device product (for example, DBLTypeProduct::PRODUCT_7960, DBLTypeProduct::PRODUCT_7940)
• Registered Cisco Unified Communications Manager name for destination device
• Destination device owner (user name that is currently logged in to the IP phone; if no explicitly logged-in user exists, this field specifies null)

Information Collected from Cisco Unified Communications Manager/CTIManager
• Source device name (MAC address)
• CallingPartyNumber (the party who placed the call; for transferred calls, the transferred party becomes the calling party)
• OriginalCalledPartyNumber (the original-called party after any digit translations occurred)
• FinalCalledPartyNumber (for forwarded calls, this specifies the last party to receive the call; for non-forwarded calls, this field specifies the original called party)
• LastRedirectDn (for forwarded calls, this field specifies the last party to redirect the call; for non-forwarded calls, this field specifies the last party to redirect, via transfer or conference, the call)
• globalCallID_callManagerId (this field distinguishes the call for CDR Analysis and Reporting (CAR))
• globalCallID_callId (this field distinguishes the call for CAR)
• CallState (Connected, On Hook)

Information Collected from the Cisco Unified Communications Manager Database
• Sampling duration - Service parameter (for example, 50 seconds)
• Sampling frequency - Service parameter (for example, 30 seconds)
• Cluster ID - Enterprise parameter

Information Collected from the User
• Category
• ReasonCode
• TimeStamp (Implicit)

Table 38-6 shows the available fields for each supported category.

---

Note

The following QRT report fields will display appropriate phone model and product names (for example, Phone That Is Running SCCP): Source Model, Source Product, Destination Model, Destination Product, and CallState.

---

### Table 38-6  QRT Fields by Supported Category

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Problems with Current Call</th>
<th>Problems with Last Call</th>
<th>Phone Recently Rebooted</th>
<th>Can't Make Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Device Name</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DN of Source Device</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IP Address of Source Device</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Device Type</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Device Owner</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Registered Cisco Unified Communications Manager for Source Device</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Model</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Product</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Stream 1 Port Number</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Codec</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Packets</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Rcvr Packets</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Table 38-6  QRT Fields by Supported Category (continued)

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Problems with Current Call</th>
<th>Problems with Last Call</th>
<th>Phone Recently Rebooted</th>
<th>Can't Make Calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Rcvr Jitter</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Rcvr Packet Lost</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Sampling Timestamp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Device Name</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DN of Destination Device</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address of Destination Device</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Device Type</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Stream 1 Port Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Codec</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Rcvr Packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Rcvr Jitter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Rcvr Packet Lost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Sampling Timestamp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Device Owner</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registered Cisco Unified Communications Manager for Destination Device</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Model</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Product</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calling Party Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Original Called Party Number</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Called Party Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Redirect DN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>globalCallID_callManagerId</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>globalCallID_callId</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sampling Duration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sampling Frequency</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Category</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Reason Code</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeStamp When Report is Submitted</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Providing Information to Users for the QRT Feature

The Cisco Unified IP Phone guides provide procedures for how to use the QRT feature on the Cisco Unified IP Phone. For more information, see the following URL for the appropriate Cisco Unified IP Phone Guide for your phone model:

Additional Information
See the “Related Topics” section on page 38-32.

Troubleshooting the QRT Feature

Cisco Unified Serviceability provides web-based tools to assist in troubleshooting Cisco Unified Communications Manager problems. Use the Cisco Unified Serviceability Trace Configuration, Alarm Configuration, and Real Time Monitoring Tool to help troubleshoot problems with QRT. See the Cisco Unified Serviceability Administration Guide for more information.

The Trace and Alarm tools work together. You can configure trace and alarm settings for Cisco CallManager services and direct alarms to local Syslogs or system diagnostic interface (SDI) log files. (SDI log files are viewable in text format only.)
You can set up traces for Cisco CallManager services on debug levels, specific trace fields, and Cisco Unified Communications Manager devices such as phones or gateways. You can also perform a trace on the alarms that are sent to the SDI trace log files.

Use the trace collection feature to collect trace files and to analyze trace data for troubleshooting problems. (The trace collection feature includes the QRT Viewer.)

The trace collection feature provides three main functions:

- Configure trace parameters
- Collect trace files
- Analyze trace data for troubleshooting problems

**Note**

Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC.

**Troubleshooting Tips**

The following examples provide some common problems and recommended actions when troubleshooting scenarios for QRT:

**Problem**  The QRT softkey is not available.

**Solution**  Ensure that you have created, configured, and assigned the softkey template to enable the QRT feature.

**Problem**  The QRT softkey is not working.

**Solution**  Ensure that the Cisco Extended Functions service, the Cisco CallManager service, the Cisco CTIManager service, and the Cisco RIS Data Collector service are operational.

**Problem**  The QRT report does not include data.

**Solution**  The system collects data from various sources, such as the user, source IP phone, destination IP phone, RIS Data Collector, Cisco Unified Communications Manager, and Cisco Unified Communications Manager databases. Check to make sure that the destination device is a supported IP phone and not a gateway or other unsupported device; otherwise, the system does not collect data from the destination device.

**Note**

For more information about Cisco Unified Serviceability tools, see the *Cisco Unified Serviceability Administration Guide*.

For information about troubleshooting Cisco Unified Communications Manager, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

**Additional Information**

See the “Related Topics” section on page 38-32.
Related Topics

- Configuration Checklist for QRT, page 38-2
- Introducing Quality Report Tool, page 38-3
- System Requirements for QRT, page 38-6
- Cisco Extended Functions Service Dependency, page 38-7
- Securing a TLS Connection to CTI, page 38-8
- How to Use QRT, page 38-9
- Interactions and Restrictions, page 38-15
- Installing and Activating QRT Functions, page 38-15
- Configuring the QRT Feature, page 38-16
- Using the QRT Viewer, page 38-25
- Providing Information to Users for the QRT Feature, page 38-30
- Troubleshooting the QRT Feature, page 38-30
- Internet Protocol Version 6 (IPv6), page 29-1
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- Device Pool Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phones, Cisco Unified Communications Manager System Guide
- Device Defaults Configuration, Cisco Unified Communications Manager Administration Guide
- Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide

Additional Cisco Documentation

- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager System Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Security Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco IP Telephony Locale Installer
- Cisco Unified IP Phone Guides
Single Sign On

The single sign on feature allows end users to log into a Windows client machine on a Windows domain, then use certain Cisco Unified Communications Manager applications without signing on again.

For more information about the single sign on feature, refer to the Cisco white paper *A complete guide for installation, configuration and integration of CUCM8.5 with Open Access Manager and Active Directory for SSO*.

This chapter, which provides information on the single sign on feature for Cisco Unified Communications Manager, contains the following topics:

- Configuration Checklist for Single Sign On, page 39-1
- Introducing Single Sign On for Cisco Unified Communications Manager, page 39-2
- System Requirements for Single Sign On, page 39-2
- Installing and Activating Single Sign On, page 39-3
- Configuring Single Sign On, page 39-3
- Related Topics, page 39-7

Configuration Checklist for Single Sign On

The single sign on feature allows end users to log into a Windows client machine, then use certain Cisco Unified Communications Manager applications without signing on again.
Table 39-1 provides a checklist for configuring single sign on in your network. Use Table 39-1 in conjunction with the “Related Topics” section on page 39-7.

For information about configuring single sign on with Cisco Unified Communication interface for Microsoft Office Communicator, refer to the Cisco Unified Communication interface for Microsoft Office Communicator documentation.

Table 39-1  Single Sign On Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Topics and Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Ensure that your environment meets the requirements described in the “System Requirements for Single Sign On” section on page 39-2</td>
</tr>
</tbody>
</table>
| **Step 2**         | Provision the OpenAM server in Active Directory, then generate keytab files.  
**Note** If your Windows version does not include the ktpass tool for generating keytab files, then you must obtain it separately. |
| **Step 3**         | Import the OpenAM server certificate into the Cisco Unified Communications Manager tomcat-trust store. |
| **Step 4**         | Configure Windows single sign on with Active Directory and OpenAM. |
| **Step 5**         | Configure client browsers for single sign on. |
| **Step 6**         | Enable single sign on in Cisco Unified Communications Manager. |

Introducing Single Sign On for Cisco Unified Communications Manager

The single sign on feature allows end users to log into Windows, then use the following Cisco Unified Communications Manager applications without signing on again:

- User Options Pages
- Cisco Unified Communication interface for Microsoft Office Communicator

System Requirements for Single Sign On

The following single sign on system requirements exist for Cisco Unified Communications Manager:

- Cisco Unified Communications Manager release 8.5(1) on each server in the cluster

The feature requires the following third-party applications:

- Microsoft Windows Server 2003 or Microsoft Windows Server 2008
- Microsoft Active Directory
Installing and Activating Single Sign On

After you install Cisco Unified Communications Manager 8.5(1), your network can support single sign on if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for Single Sign On” section on page 39-1.

Configuring Single Sign On

This section contains information on the following topics:

- Configuring OpenAM, page 39-3
- Configuring Windows Single Sign On with Active Directory and OpenAM, page 39-4
- Configuring Client Browsers for Single Sign On, page 39-4

Tip

Before you configure single sign on, review the “Configuration Checklist for Single Sign On” section on page 39-1.

Configuring OpenAM

Perform the following tasks using OpenAM:

- Configure policies in OpenAM for the following:
  - CUCM User and UDS web application
  - Query Parameters
- Configure a J2EE Agent Profile for Policy Agent 3.0.
- Configure a Windows Desktop SSO login module instance.

The single sign on feature uses Active Directory and OpenAM in combination to provide single sign on access to client applications.

These third party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, Cisco Unified Communications Manager, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- No third-party products may be installed on the Cisco Unified Communications Manager server.
- The clocks of all the entities participating in SSO must be synchronized.

See the third-party product documentation for more information about those products.
• Configure “Login Form URI” and “OpenAM Login URL” for the PA.
• Disable local user profiles.

Importing the OpenAM Certificate into Cisco Unified Communications Manager

Because communication between Cisco Unified Communications Manager and OpenAM is secure, you must obtain the OpenAM security certificate and import it into the Cisco Unified Communications Manager tomcat-trust store. Configure the OpenAM certificate to be valid for 5 years.

For information about importing certificates, see the Cisco Unified Communications Operating System Administration Guide.

Configuring Windows Single Sign On with Active Directory and OpenAM

This section describes how to configure Windows single sign on with Active Directory and OpenAM. This procedure allows Cisco Unified Communications Manager to authenticate with Active Directory.

Procedure

Step 1 In Active Directory, create a new user with the OpenAM Enterprise host name (without the domain name) as the User ID (login name).

Step 2 Create keytab files on the Active Directory server.

Step 3 Export the keytab files to the OpenAM system.

Step 4 In OpenAM, create a new authentication module instance with the following configuration:

• The type is Windows Desktop SSO.
• The realm attributes are determined as follows:
  - Service Principal: Enter the principal name that you used to create the keytab file.
  - Keytab File Name: Enter the path where you imported the keytab file.
  - Kerberos Realm: Enter the domain name.
  - Kerberos Server Name: Enter the FQDN of the Active Directory server.
  - Authentication level: Enter 22.

Configuring Client Browsers for Single Sign On

To use single sign on for a browser-based client application, you must configure the web browser. The following sections describe how to configure client browsers to use single sign on:

• Configuring Internet Explorer for Single Sign On, page 39-5
• Configuring FireFox for Single Sign On, page 39-5
Configuring Internet Explorer for Single Sign On

The single sign on feature supports Windows clients running Internet Explorer version 6.0 and higher. Do the following tasks to configure Internet Explorer to use single sign on:

- Select the Integrated Windows Authentication option.
- Create a custom security level configured as follows:
  - Select the Automatic Logon Only in Intranet Zone option
  - Select all of the options for sites.
  - Add OpenAM to the local zone, if it not already added.
- Do the following tasks for Internet Explorer 8.0 running on Windows 7:
  - Disable Protected Mode.
  - Under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA, add DWORD value SuppressExtendedProtection - 0x02.

Configuring FireFox for Single Sign On

The single sign on feature supports Windows clients running FireFox version 3.0 and higher. To configure Firefox to use single sign on, enter the trusted domains and URLs that are permitted to engage in SPNEGO Authentication with the browser into the network.negotiate-auth.trusted-uris preference.

Running CLI Commands for Single Sign On

The following sections describe the CLI commands that configure single sign on:

- `utils sso enable`, page 39-5
- `utils sso disable`, page 39-6
- `utils sso status`, page 39-7

**utils sso enable**

This command enables and configures single sign on.

**Command Syntax**

```
utils sso enable
```

**Usage Guidelines**

This command starts a single sign on configuration wizard. You get prompted for the information described in Table 39-2. Answer each prompt, then press **Enter** to continue.

**Caution**

Enabling single sign on restarts the Cisco Unified Communications Manager web server (Tomcat).

You must run this command on all nodes in a cluster.
Chapter 39      Single Sign On

Configuring Single Sign On

Example

admin:utils sso enable
***** W A R N I N G *****
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
Enter URL of the Open Access Manager (OpenAM) server:
https://ssoserver.cisco.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: CUCMUser
Enter the password of the profile name: ********
Enter the login module instance name configured for Windows Desktop SSO: CUCMUser
Validating connectivity and profile with AM Server:
https://ssoserver.cisco.com:8443/opensso
Valid profile
Enabling SSO ... This will take upto 5 minutes
SSO Enable Success

Please make sure to execute this command on all the nodes in the cluster.

utils sso disable

This command disables single sign on.

Command Syntax
utils sso disable

Usage Guidelines

Caution
Disabling single sign on restarts the Cisco Unified Communications Manager web server (Tomcat).

You must run this command on all nodes in a cluster.

Table 39-2      Single Sign On Configuration Wizard Prompts

<table>
<thead>
<tr>
<th>Information That the Prompt Requests</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL of the Open Access Manager (OpenAM) server</td>
<td>The URL that you configured for the OpenAM server.</td>
</tr>
<tr>
<td>Relative path where the policy agent should be deployed</td>
<td>Enter the path on the Cisco Unified Communications Manager where the policy agent will get deployed. This path is relative to the “agentapp” directory. This path must match the path that you configured for the J2EE Agent Profile for Policy Agent 3.0.</td>
</tr>
<tr>
<td>Name of the profile configured for this policy agent</td>
<td>The name of the profile that you created for this policy agent in OpenAM.</td>
</tr>
<tr>
<td>Password of the profile.</td>
<td>—</td>
</tr>
<tr>
<td>Login module instance name configured for Windows Desktop SSO</td>
<td>The name of the login module instance for Windows Desktop SSO that you configured in OpenAM.</td>
</tr>
</tbody>
</table>
utils sso status

This command displays the status and configuration parameters of single sign on.

Command Syntax
utils sso status

Related Topics

- Configuration Checklist for Single Sign On, page 39-1
- Introducing Single Sign On for Cisco Unified Communications Manager, page 39-2
- System Requirements for Single Sign On, page 39-2
- Installing and Activating Single Sign On, page 39-3
- Configuring Single Sign On, page 39-3
INDEX

A

AAR
  See automated alternate routing (AAR)
access, restricting with partitions 6-21
access control
  MLPP numbering plan
    example (figure) 35-25
    explained 35-25
  precedence patterns
    example (figure) 35-25
    explained 35-25
access lists
  configuration 14-36
  configuration settings (table) 14-36
  member details configuration settings (table) 14-38
ad hoc conference
  interactions with logical partitioning 32-27
adjunct licensing 30-9
agent call
  barging or monitoring 34-12
alert, call pickup 6-21
alternate party diversion (APD)
  example (figure) 35-14
  explained 35-13
announcements
  blocked precedence 35-23
  blocked precedence (figure) 35-23
  busy station 35-24
  MLPP 35-21
  unauthorized precedence 35-22
  unauthorized precedence (figure) 35-23
annunciator

IPv6 29-17
application dial rules
  configuring for Web Dialer 17-11
application users
  configuring for Web Dialer 17-9
assisted directed call park 5-29
audio sources
  configuring 36-18
  creating for MOH 36-12
  for MOH 36-12
  managing for MOH 36-13
  multicast 36-13
  storing for MOH 36-12
  unicast 36-13
auto call pickup
  described 6-17
  interactions with Cisco Unified Mobility 14-28
automated alternate routing (AAR)
  MLPP interaction 35-32

B

bandwidth
  insufficient with AAR for MLPP 35-32
Barge
  interactions with logical partitioning 32-34
  barge
    activating with built-in conference bridge 1-16
    built-in and shared conference bridge differences (table) 1-6
    configuration checklist (table) 1-2
    configuring 1-17
    described 1-6
installing and activating 1-16
interactions and restrictions 1-12
intercom usage 28-6
overview 1-1
party entrance tone 1-9
PLAR support 1-13
related topics 1-17
service parameters 1-17
softkey 1-8
system requirements 1-11

BIB call information and call display 34-58
BLF
configuring for directed call park 5-27
directed call park configuration settings 5-27
BLF/SpeedDial
buttons 37-20
configuration settings (table) 5-27, 37-21
configuring 37-20
built-in bridge
See BIB
built-in conference bridge, barge 1-16
busy lamp field call pickup
configuration checklist (table) 6-7
described 6-16
example 6-17

C

Call Back
additional information for Call Back notification with phones that are running SIP 2-8
configuration checklist 2-1
description 2-3
interactions and restrictions 2-7
interactions with Call Forward, iDivert, and Voice-Mail System features 2-8
overview 2-1
setting service parameters 2-12
softkey template 2-9
suspend/resume functionality 2-5
system requirements 2-6
understanding 2-3
call classification configuration settings (table) 23-8
call control discovery 3-1
call display restrictions
configuration checklist (table) 4-1
configuring 4-6
configuring in translation pattern 28-26
configuring phones for 4-8
enabling 4-3
interactions
call park 4-5
conference 4-6
conference list 4-6
extension mobility 4-6
listed 4-5
voice mail 4-6
introduction 4-2
overview 4-1, 4-3
related topics 4-14
sample call flow (figure) 4-13
sample configurations
calling search spaces 4-10
call park 4-13
devices 4-10
gateways 4-10
listed 4-9
translation patterns 4-11
scenarios 4-4
service parameter for connected number display 4-14
system requirements 4-4
translation patterns for 4-7
with Cisco Extension Mobility 9-15
called digits transformation (figure) 31-12
called party
transformations
and local route groups 31-11
call forward
MLPP interaction 35-30

call forwarding
   interactions with logical partitioning 32-23

calling party normalization
   activating 8-15
   BAT support 8-12
   Call Detail Record support 8-12
   calling party number type 8-17
   calling party transformation CSS 8-25
   CAR support 8-12
   Cisco Extension Mobility support 8-13
   Cisco Unified Communications Manager Assistant support 8-12
   Cisco Unity Connection support 8-12
   Cisco Unity support 8-12
   configuration checklist 8-1
   configuring 8-15
   device mobility support 8-13
   forwarding calls 8-11
   globalizing described 8-5
   information for end users 8-26
   installing 8-15
   interactions 8-11
   localizing, described 8-7
   mapping global number to local variant 8-9
   phone support 8-10
   related topics 8-27
   restrictions 8-14
   service parameters 8-15
   system requirements 8-10
   transferring calls 8-11

calling party transformation patterns 8-7

calling search spaces
   Cisco Unified Communications Manager Assistant
      configuration tips 11-22
   configure display in drop-down list box 28-36
   partition limitations 28-18
   SUBSCRIBE (for Presence) 37-11, 37-14

call monitoring

See monitoring

call park
   configuration checklist (table) 5-2
   configuration settings (table) 5-14
   configuring 5-11
   configuring a number 5-13, 5-24
   deleting a number 5-15
   directed
      via DTMF with Cisco Unified Mobility 14-15
   example with MOH 36-8
   finding a number 5-11
   installing and activating 5-10
   interactions 5-8
   interactions with logical partitioning 32-30
   interaction with call display restrictions 4-5
   introduction 5-4
   overview 5-1
   restrictions 5-10
   setting service parameters 5-11
   system requirements 5-7
   usage example 5-5

call pickup
   activating 6-25
   auto
      described 6-17
      interactions with Cisco Unified Mobility 14-28
   busy 6-18
   busy lamp field
      configuration checklist (table) 6-7
      described 6-16
   call pickup group
      assigning to a directory number 6-33
      defining a pickup group for other group pickup 6-33
   configuration checklist (table) 6-1
   configuring 6-26
   directed
      configuration checklist (table) 6-5
      described 6-12
Index

examples 6-13

group call pickup
  described 6-11
installing 6-25

interactions
  call accounting 6-24
  calling search space 6-24
  dependency records 6-25
  listed 6-24
  partitions 6-24
  route plan report 6-24
  time of day 6-24
interactions and restrictions 6-23
interactions with logical partitioning 32-29
introducing 6-10
no answer 6-18
no bandwidth 6-18
notification 6-21
other group
  configuration checklist (table) 6-3
    described 6-12
overview 6-1
phone feature described 6-11
related topics 6-34
restricting access 6-21
restrictions
  listed 6-25
  service parameters 6-26
  system requirements 6-22
  using with partitions 6-21
call pickup group
  configuration settings (table) 6-29
  configuring 6-27, 6-28
  deleting 6-32
  finding 6-27
call preservation
  with intercom 28-6
  with MLPP 35-32
call recording

See recording
call throttling
  introduction 7-1
  related topics 7-3
  troubleshooting 7-2
call transfer
  interactions with logical partitioning 32-24
  MLPP interaction 35-31
call waiting
  MLPP interaction 35-31
cBarge
  activating with shared conference bridge 1-16
  interactions with logical partitioning 32-34
  party entrance tone 1-9
  PLAR support 1-13
  softkey 1-9

CDR
  recording for precedence calls 35-30

CEF
  See Cisco Extended Functions
channel nonpreemptable 35-17
Cisco Customer Response Platform components 13-5
Cisco Extended Functions
  activating for QRT 38-22
  DB Change Notifier 38-6
  DBL library 38-5
  multiple applications in a cluster 38-8
  QBEHelper 38-5
  redundancy manager 38-6
  screen helper and dictionary 38-5
  SDI Trace and Alarm 38-6
  service architecture 38-4
  service architecture (figure) 38-5
  service dependency 38-7
  service dependency (figure) 38-7
  service parameters for QRT 38-24
Cisco Extension Mobility
  adding the Cisco Extension Mobility service 9-19
configuration checklist (table) 9-1
configuration example 9-18
configuration guidelines 9-17
configuring 9-17
creating a default device profile for each Cisco Unified IP Phone type 9-26
creating the device profile for a user 9-28
description 9-6
device profiles
  default 9-6
  understanding 9-5
  user 9-6
equivalency 9-11
illustrated (figure) 9-7
information for users 9-35
installing 9-17
interactions
  bulk administration tool 9-14
  call display restrictions 9-15
  Cisco Unified Communications Manager Assistant 9-15
  intercom 9-15
  IPv6 9-16
  listed 9-14
  Presence 37-11
  Pv6 29-17
  services that are running on the same server 9-14
interactions and restrictions 9-14
interactions with logical partitioning 32-31
intercom interactions 28-7
introducing 9-5
login and logout behavior 9-8
login call flow 9-9
logout call flow 9-10
overview 9-1
related topics 9-35
restrictions 9-16
setting service parameters (table) 9-20
subscribing phones 9-32
system requirements 9-13
user device profile, associating 9-31
using 9-35
Cisco Extension Mobility Cross Cluster
  See Extension Mobility Cross Cluster
Cisco IPMA
  See Cisco Unified Communications Manager Assistant
Cisco IP Manager Assistant service
  understanding 11-7, 12-6
Cisco Mobile clients 16-1
Cisco Unified Communications Manager
  IPv6 29-18
  MOH servers 36-10
Cisco Unified Communications Manager Assistant
  architecture overview 11-6, 12-5
  assistant console dialog options 11-43, 12-30
  assistant console interface 11-9, 12-7
  assistant interfaces 11-10, 12-8
  bulk administration tool 11-13, 12-11
  calling party normalization 11-14, 12-11
  calling search space and partitions, configuration tips 11-22
Cisco Unified IP Phone interface 11-10, 12-8
Cisco Unified IP Phone Services, configuration tips 11-29
configuration checklist for proxy line support (table) 11-2
configuration checklist with shared line support (table) 12-2
configuration wizard for proxy line 11-19
configuring assistant phones, tips 11-31
configuring assistant proxy and incoming intercom lines 11-38
configuring manager and assigning assistant for proxy line 11-34
configuring manager and assigning assistant for shared line 12-22
configuring manager phones, tips 11-30
configuring manager primary and incoming intercom lines 11-34, 12-22
configuring shared and incoming intercom lines for assistant 12-25
database access architecture, understanding 11-10, 12-8
deleting assistant information 11-39, 12-27
deleting manager information 11-36, 12-24
dial rules configuration 11-41, 12-28
extension mobility 11-14, 12-28
installing and activating 11-17, 12-15
installing the assistant console application 12-29
interactions 11-13
intercom 11-16, 12-14
intercom usage 28-6
IPMASecureSysUser 11-28, 12-19
IPv6 11-14, 12-12
manager and assistant configuration 12-21
manager and assistant phone configuration 11-29, 12-19
manager assistant administration interface 11-11, 12-9
manager interfaces 11-10, 12-8
message waiting indicator 11-16
more information 12-31
multilevel precedence and preemption 11-15
Multilevel Precedence and Preemption (MLPP) 12-13
phones, configuration tips 11-33, 12-21
providing information to managers and assistants 11-41, 12-28
reporting tools 11-14, 12-12
restrictions 11-13, 11-16, 12-14
route point configuration tips 11-23
scalability 11-27, 12-18
security 11-28, 12-19
setting service parameters 11-24, 12-16
softkeys 11-11, 12-9
starting the Cisco IP Manager Assistant service 11-29, 12-19
supported devices 11-12, 12-10
system configuration with proxy line 11-18
system requirements for proxy line support 11-12
system requirements for shared line support 12-10
time-of-day routing 11-16
updating assistant information 11-40, 12-27
updating manager information 11-37, 12-24
with proxy line support 11-1
with shared line support 12-1
Cisco Unified Communications Manager Auto-Attendant
Cisco Unified Communications Manager and the CRS engine 13-6
components 13-5
configuration checklist (table) 13-2
description 13-1
installing 13-6
managing 13-6
overview 13-4
understanding 13-3
Cisco Unified IP Phones
subscribing to Cisco Extension Mobility 9-32
Cisco Unified IP Phone Services
Cisco Unified Communications Manager Assistant
configuration tips 11-29
Cisco Unified Mobile Communicator
and Cisco Unified Mobility
configuration checklist (table) 15-8
configuration details 15-9
described 15-7
integration overview 15-1
Cisco Unified Mobility
access list configuration 14-36
access list configuration settings (table) 14-36
access list member detail configuration settings (table) 14-38
associating a DN with a remote destination profile 14-43
benefits 14-7
Cisco Unified Mobile Communicator
described 15-7
configuration checklist (table) 14-2
configuring 14-35
configuring directory number for MVA 14-48
configuring softkeys 14-61
definitions (table) 14-5
delayed anchoring 15-15
described 14-1
desktop call pickup 14-10
dial-via-office forward 15-11
directed call park via DTMF 14-15
feature benefits 14-7
handoff mobility configuration
settings (table) 14-57
intelligent session control 14-17
interactions
auto call pickup 14-28
intelligent session control with session handoff 14-29
licensing 14-29
listed 14-28
local route groups 14-29, 31-15
number of supported calls 14-30
interactions and limitations 14-27, 15-18
interactions with logical partitioning 32-32
introducing 14-4, 15-4
IPv6 29-19
limitations
listed 14-30
list of features 14-6
midcall enterprise feature support using DTMF 14-12
migrating from Cisco Unified MobilityManager 14-35
mobile connect 14-8
mobile voice access 14-11
mobile voice access configuration settings (table) 14-49
mobility enterprise feature configuration
settings (table) 14-56
mobility profile configuration
settings (table) 14-58
related topics 14-62, 15-20
remote destination configuration settings (table) 14-44
remote destination profile
configuring 14-39
remote destination profile configuration settings (table) 14-39
remote destinations
configuring 14-43
send call to mobile phone 14-10
SIP URI dialing 14-16
system requirements 14-34
time-of-day access
configuration checklist (table) 14-13
described 14-12
important notes 14-14
two-stage dialing 14-12
use case scenarios
dial-via-office forward 15-13, 15-16
dial-via-office reverse callback 15-16
directed call park via DTMF 14-23
intelligent session control 14-24
listed 14-21, 15-15
mobile connect 14-21
mobile voice access 14-22
time-of-day access 14-22
with Cisco Unified Mobile Communicator
overview 15-1
restrictions 15-18
with Cisco Unified Mobility Advantage
Cisco Unified Mobile Communicator configuration checklist (table) 15-8
Cisco Unified Mobile Communicator configuration details 15-9
configuration checklist (table) 15-2
configuring 15-19
definitions (table) 15-5
dial-via-office reverse callback 15-10
introducing 15-4
list of features 15-4
overview 15-1
restrictions 15-18
system requirements 15-19
Index

Cisco Unified Mobility Advantage
integration overview 15-1
Cisco Unified MobilityManager
migrating to Cisco Unified Mobility 14-35
Cisco Unity
IPv6 29-17
Cisco Unity Connection
IPv6 29-17
Cisco Web Dialer
IPv6 29-18
See Web Dialer
client matter codes
BAT usage 18-5
CAR usage 18-6
configuration settings (table) 18-7
CTI, JTAPI, and TAPI usage 18-6
described 18-2
enabling for route patterns 18-8
installation 18-6
interactions 18-4
requirements 18-6
restrictions 18-4
system requirements 18-6
user information 18-11
codecs
for monitoring and recording calls (figure) 34-56
code yellow state 7-1
common network facility preemption
example (figure) 35-18
example with retry timer Tr (figure) 35-19
explained 35-17
conference list
interaction with call display restrictions 4-6
conferences
IPv6 29-18
CTI
event delivery for monitoring and recording (figure) 34-59
interactions with logical partitioning 32-36
intercom interactions 28-6
requirements for monitoring and recording 34-59
securing TLS connection 38-8
CTI route points
Cisco Unified Communications Manager Assistant configuration tips 11-23
Customer Response Solutions, installing 13-6
custom phone rings
creating 19-3
customizing files 19-2
introduction 19-1
overview 19-1
PCM file requirements 19-3
database scalability 36-10
default device profiles
creating for each Cisco Unified IP Phone type 9-26
delayed anchoring
with Cisco Unified Mobility 15-15
deny handling
for logical partitioning 32-18
device mobility
and calling party normalization 8-13, 20-8
and IPv4 20-8
and IPv6 20-8
configuration checklist 20-2
configuration tips 20-11
configuring 20-10
enabling/disabling 20-12
feature interactions 20-8
feature restrictions 20-8
installing 20-10
introducing 20-3
IPv6 29-18
more information 20-21
network considerations 20-7
operations 20-3
overview 20-1
system requirements 20-9
viewing roaming parameters 20-21
device mobility groups
configuration settings (table) 20-17
configuring 20-16
deleting 20-17
finding 20-15
device mobility info
configuration settings (table) 20-19
configuring 20-19
deleting 20-20
finding 20-18
device profiles
and Cisco Extension Mobility 9-5
creating for a Cisco Extension Mobility user 9-28
default for Cisco Extension Mobility 9-6
for a Cisco Extension Mobility user 9-31
user for Cisco Extension Mobility 9-6
DHCP
IPv6 29-10
dial-via-office forward
with Cisco Unified Mobility 15-11
dial-via-office reverse callback
with Cisco Unified Mobility 15-10
directed call park
BLF configuration settings 5-27
configuration checklist (table) 5-3
configuration settings (table) 5-26
configuring BLF/Directed Call Park buttons 5-27
deleting a number 5-29
finding a number 5-23
installing and activating 5-23
interactions 5-20
interactions with logical partitioning 32-30
introduction 5-19
overview 5-1
restrictions 5-22
setting service parameters 5-23
synchronizing configuration to applicable devices 5-28
system requirements 5-20
usage example 5-19
via DTMF
with Cisco Unified Mobility 14-15
directed call pickup
basic completion (figure) 6-13
basic setup (figure) 6-13
configuration checklist (table) 6-5
described 6-12, 6-13
multiple-calls completion (figure) 6-16
multiple-calls setup (figure) 6-16
rejection (figure) 6-14, 6-15
directory number
assigning a call pickup group 6-33
directory numbers
calling search space list 28-36
for intercom
configuration overview 28-29
DND
adding to common phone profiles 21-11
architecture overview 21-3
configuration checklist 21-1
configuring 21-7
described 21-1
device parameters (table) 21-9
feature key 21-9
hardware requirements 21-4
high priority call with DND ringer off enabled on a shared line (figure) 21-15
incoming call alert settings 21-2
installing and activating 21-7
interactions
callback 21-6
extension mobility 21-7
hold reversion and intercom 21-6
hunt list 21-6
listed 21-5
related topics 23-9
restrictions 23-5, 23-6
route pattern configuration 23-9
service parameters 23-7
system requirements 23-5
transferring external calls to an external party (figure) 23-4
trunk configuration 23-8

time-of-day routing 11-16
understanding architecture 11-6, 12-5
understanding database access architecture 11-10
understanding database and directory access architecture 12-8
device mobility 20-1
directed call park 5-1
external call transfer restrictions 23-1
hold reversion 25-1
immediate divert 27-1
malicious call ID (MCID) 33-2
Multilevel Precedence and Preemption (MLPP) using with Cisco Unified Communications Manager Assistant 12-13
Presence 37-1, 37-4
privacy 1-1
QRT 38-1, 38-16
Single Sign on 39-1
Web Dialer 17-1

features
barge 1-1
call display restrictions 4-1
call park 5-1
Cisco Extension Mobility
bulk administration tool 9-14
Cisco Unified Communications Manager Assistant
assistant console interface 11-9, 12-7
assistant interfaces 11-10, 12-8
bulk administration tool 11-13, 12-11
calling party normalization 11-14, 12-11
calling search space and partitions 11-22
Cisco Unified IP Phone interface 11-10, 12-8
Cisco Unified IP Phone Services 11-29
configuration checklist for proxy line support (table) 11-2
extension mobility 11-14, 12-12
intercom 11-16, 12-14
manager assistant administration interface 11-11, 12-9
manager interfaces 11-10, 12-8
message waiting indicator 11-16
multilevel precedence and preemption 11-15
Multilevel Precedence and Preemption (MLLP) 12-13
phones 11-33, 12-21
reporting tools 11-14, 12-12
route point 11-23
softkeys 11-11, 12-9

file format, Ringlist.xml 19-2
firewalls and one-way media (figure) 34-57
fixed audio source
configuration settings (table) 36-25
configuring 36-23, 36-24
deleting 36-24
forced authorization codes
BAT usage 18-5
CAR usage 18-6
configuration settings (table) 18-9
CTI, JTAPI, and TAPI usage 18-6
described 18-3
enabling for route patterns 18-10
installation 18-6
interactions 18-4
requirements 18-6
restrictions 18-4
system requirements 18-6
<table>
<thead>
<tr>
<th><strong>Index</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>user information</strong></td>
</tr>
<tr>
<td><strong>forwarding</strong></td>
</tr>
<tr>
<td><strong>dial-via-office with Cisco Unified Mobility</strong></td>
</tr>
<tr>
<td><strong>forwarding</strong></td>
</tr>
<tr>
<td><strong>local route groups</strong></td>
</tr>
</tbody>
</table>

**G**

<table>
<thead>
<tr>
<th><strong>gateways</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv6</strong></td>
</tr>
<tr>
<td><strong>geolocation filters</strong></td>
</tr>
<tr>
<td>configuration checklist (table)</td>
</tr>
<tr>
<td>configuration settings (table)</td>
</tr>
<tr>
<td>configuring</td>
</tr>
<tr>
<td>deleting</td>
</tr>
<tr>
<td>examples (table)</td>
</tr>
<tr>
<td>finding</td>
</tr>
<tr>
<td>introducing</td>
</tr>
<tr>
<td>logical partitioning use</td>
</tr>
<tr>
<td>related topics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>geolocations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>and route lists</strong></td>
</tr>
<tr>
<td><strong>and shared lines</strong></td>
</tr>
<tr>
<td><strong>characteristics</strong></td>
</tr>
<tr>
<td>configuration checklist (table)</td>
</tr>
<tr>
<td>configuration settings (table)</td>
</tr>
<tr>
<td>configuring</td>
</tr>
<tr>
<td>deleting</td>
</tr>
<tr>
<td>examples</td>
</tr>
<tr>
<td>examples (table)</td>
</tr>
<tr>
<td>finding</td>
</tr>
<tr>
<td>identifiers</td>
</tr>
<tr>
<td>logical partitioning usage</td>
</tr>
<tr>
<td>interactions</td>
</tr>
<tr>
<td>intercluster trunk error handling with location conveyance</td>
</tr>
<tr>
<td>introducing</td>
</tr>
<tr>
<td>location conveyance feature interactions</td>
</tr>
<tr>
<td>logical partitioning feature interactions with midcall change</td>
</tr>
<tr>
<td>logical partitioning handling</td>
</tr>
<tr>
<td>logical partitioning use</td>
</tr>
<tr>
<td>overview</td>
</tr>
<tr>
<td>related topics</td>
</tr>
<tr>
<td>SIP trunk error handling with location conveyance</td>
</tr>
<tr>
<td>source information</td>
</tr>
<tr>
<td><strong>globalizing calling party number</strong></td>
</tr>
<tr>
<td>activating</td>
</tr>
<tr>
<td>BAT support</td>
</tr>
<tr>
<td>Call Detail Record support</td>
</tr>
<tr>
<td>calling party number type</td>
</tr>
<tr>
<td>CAR support</td>
</tr>
<tr>
<td>Cisco Extension Mobility support</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Assistant support</td>
</tr>
<tr>
<td>Cisco Unity Connection support</td>
</tr>
<tr>
<td>Cisco Unity support</td>
</tr>
<tr>
<td>configuration checklist</td>
</tr>
<tr>
<td>configuring</td>
</tr>
<tr>
<td>described</td>
</tr>
<tr>
<td>device mobility support</td>
</tr>
<tr>
<td>example</td>
</tr>
<tr>
<td>forwarding</td>
</tr>
<tr>
<td>gateway support</td>
</tr>
<tr>
<td>information for end users</td>
</tr>
<tr>
<td>installing</td>
</tr>
<tr>
<td>interactions</td>
</tr>
<tr>
<td>mapping global number to local variant</td>
</tr>
<tr>
<td>phone support</td>
</tr>
<tr>
<td>related topics</td>
</tr>
<tr>
<td>restrictions</td>
</tr>
<tr>
<td>service parameters</td>
</tr>
<tr>
<td>system requirements</td>
</tr>
<tr>
<td>transferring</td>
</tr>
<tr>
<td><strong>group call pickup</strong></td>
</tr>
<tr>
<td>configuration checklist (table)</td>
</tr>
<tr>
<td>described</td>
</tr>
</tbody>
</table>
H

H.323
   IPv6  29-18
H.323 gateway
   configuring for enterprise feature access options  14-50
   configuring for system remote access
      no hairpinning  14-50
      using hairpinning  14-53
hold reversion
   alerting operations (table)  25-4
   call focus operations  25-5
   call focus priority  25-12
   configuration checklist (table)  25-1
   configuration tips  25-12
   configuring  25-11
   configuring call focus priority  25-13
   configuring call reversion timer settings  25-14
   description  25-3
   examples  25-3, 25-6
   installing  25-11
   interactions
      call park  25-9
      CTI applications  25-10
      listed  25-9
      MLPP  25-10
      music on hold  25-9
   introducing  25-2
   more information  25-16
   overview  25-1
   providing information to users  25-15
   restrictions  25-10
   retrieving reverted calls  25-5
   supported devices  25-8
   system requirements  25-8
   timer deactivation  25-6
   timers  25-12
   troubleshooting  25-15

Hotline
   activating  26-7
   call and receive settings  26-4
   call screening  26-4
      using calling party number routing  26-5
      using CSS and partitions  26-4
   configuration checklist (table)  26-1
   configuration settings in Cisco Unified CM Administration (table)  26-9
   enterprise parameters (table)  26-7
   installing  26-7
   overview  26-3
   related topics  26-12
   service parameters (table)  26-7
   system requirements  26-6
   hotline
      supported devices  26-6
   hunt pilots
      interactions with logical partitioning  32-35

I

Immediate divert
   call-processing requirements  27-4
   configuration checklist (table)  27-1
   configuring  27-10
   installing and activating  27-10
   interactions
      call detail records  27-8
      call forward  27-8
      conference  27-8
      hunt list  27-8
      listed  27-8
      MLPP  27-8
   interactions and restrictions  27-7
   introducing  27-2
   overview  27-1
   phone display messages  27-5
   related topics  27-11
requirements for incoming calls 27-4
requirements for outgoing calls 27-5
restrictions 27-9
scenarios 27-6, 27-7
setting service parameters 27-10
softkey requirements 27-4
system requirements 27-3
using 27-5
indication enabled 35-12
insufficient bandwidth, AAR for MLPP 35-32
intercluster trunks
configuration requirement for logical partitioning 32-21
location conveyance 24-22
logical partitioning interaction with geolocation conveyance 32-19
intercom
and IPv4 28-7
and IPv6 28-7
barge usage 28-6
calling search spaces
configuration overview 28-15
configuration settings (table) 28-17
configuring 28-16
deleting 28-19
finding 28-15
call preservation 28-6
Cisco Extension Mobility interactions 28-7
Cisco Unified Communications Manager Assistant 11-16
Cisco Unified Communications Manager Assistant usage 28-6
configuration checklist (table) 28-1
configuring 28-8
CTI interactions 28-6
described 28-1
directory numbers
configuration overview 28-28, 28-29
configuration settings (table) 28-31
configuring 28-30
finding 28-29
DND usage 28-6
installing and activating 28-7
interactions 28-5
IP phones supported 28-4
IPv6 29-19
overview 28-2
partitions
calling search space limitations (table) 28-13
configuration settings (table) 28-11
configuring 28-14
deleting 28-14
finding 28-9
restrictions 28-5
SRST usage 28-6
system requirements 28-4
translation patterns
configuration overview 28-20
configuration settings (table) 28-22
configuring 28-21
deleting 28-28
finding 28-20
using 28-38
with Cisco Extension Mobility 9-15
intercom directory numbers
synchronizing configuration to applicable devices 28-37
intercom partitions
synchronizing configuration to applicable devices 28-13
IPMA, Cisco
See Cisco Unified Communications Manager Assistant
IPv6
activating 29-21
additional Cisco documentation 29-32
annunciator 29-17
call admission control 29-6
call detail records 29-17
call processing 29-6
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Certificate Authority Proxy Function</td>
<td>29-17</td>
</tr>
<tr>
<td>Cisco Extension Mobility</td>
<td>29-17</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>29-18</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager server</td>
<td>29-6</td>
</tr>
<tr>
<td>Cisco Unified IP Phones</td>
<td>29-8</td>
</tr>
<tr>
<td>Cisco Unified Mobility</td>
<td>29-19</td>
</tr>
<tr>
<td>Cisco Unity</td>
<td>29-17</td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>29-17</td>
</tr>
<tr>
<td>Cisco Web Dialer</td>
<td>29-18</td>
</tr>
<tr>
<td>CLI commands</td>
<td>29-21</td>
</tr>
<tr>
<td>conferences</td>
<td>29-18</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>29-2</td>
</tr>
<tr>
<td>configuration settings in Cisco Unified CM Administration (table)</td>
<td>29-27</td>
</tr>
<tr>
<td>CTI</td>
<td>29-5</td>
</tr>
<tr>
<td>device mobility</td>
<td>29-18</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>29-10</td>
</tr>
<tr>
<td>DNS</td>
<td>29-11</td>
</tr>
<tr>
<td>DSCP</td>
<td>29-18</td>
</tr>
<tr>
<td>enterprise parameters (table)</td>
<td>29-25</td>
</tr>
<tr>
<td>Ethernet IPv6 configuration settings (table)</td>
<td>29-21</td>
</tr>
<tr>
<td>gateways</td>
<td>29-12</td>
</tr>
<tr>
<td>H.323 devices</td>
<td>29-18</td>
</tr>
<tr>
<td>installing</td>
<td>29-21</td>
</tr>
<tr>
<td>interactions</td>
<td>3-16, 29-16</td>
</tr>
<tr>
<td>intercom</td>
<td>29-19</td>
</tr>
<tr>
<td>media termination points (MTP)</td>
<td>29-12</td>
</tr>
<tr>
<td>monitoring and recording</td>
<td>29-19</td>
</tr>
<tr>
<td>music on hold</td>
<td>29-19</td>
</tr>
<tr>
<td>overview</td>
<td>3-5, 22-5, 29-5</td>
</tr>
<tr>
<td>phone web browser</td>
<td>29-20</td>
</tr>
<tr>
<td>Quality Report Tool (QRT)</td>
<td>29-19</td>
</tr>
<tr>
<td>Real-Time Monitoring Tool (RTMT)</td>
<td>29-18</td>
</tr>
<tr>
<td>related topics</td>
<td>3-47, 29-32</td>
</tr>
<tr>
<td>restrictions</td>
<td>3-16, 29-16</td>
</tr>
<tr>
<td>RSVP</td>
<td>29-19</td>
</tr>
<tr>
<td>SDL</td>
<td>29-19</td>
</tr>
<tr>
<td>service parameters (table)</td>
<td>29-25</td>
</tr>
<tr>
<td>SIP Phones</td>
<td>29-19</td>
</tr>
<tr>
<td>SIP trunks</td>
<td>29-13</td>
</tr>
<tr>
<td>system requirements</td>
<td>29-16</td>
</tr>
<tr>
<td>T.38 Fax</td>
<td>29-20</td>
</tr>
<tr>
<td>TFTP server</td>
<td>29-15</td>
</tr>
<tr>
<td>transfer</td>
<td>29-20</td>
</tr>
<tr>
<td>troubleshooting</td>
<td>29-32</td>
</tr>
<tr>
<td>video</td>
<td>29-20</td>
</tr>
<tr>
<td>J</td>
<td></td>
</tr>
<tr>
<td>join</td>
<td></td>
</tr>
<tr>
<td>interactions with logical partitioning</td>
<td>32-27</td>
</tr>
<tr>
<td>join across lines</td>
<td></td>
</tr>
<tr>
<td>interactions with logical partitioning</td>
<td>32-27</td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>license capabilities assignment</td>
<td></td>
</tr>
<tr>
<td>configuration settings (table)</td>
<td>30-18</td>
</tr>
<tr>
<td>configuring for multiple users</td>
<td>30-20</td>
</tr>
<tr>
<td>configuring for one user</td>
<td>30-20</td>
</tr>
<tr>
<td>finding</td>
<td>30-19</td>
</tr>
<tr>
<td>licensing</td>
<td></td>
</tr>
<tr>
<td>adjunct devices</td>
<td>30-9</td>
</tr>
<tr>
<td>alarms</td>
<td>30-21</td>
</tr>
<tr>
<td>applications</td>
<td>30-9</td>
</tr>
<tr>
<td>calculations</td>
<td>30-12</td>
</tr>
<tr>
<td>Cisco IP Communicator</td>
<td>30-9</td>
</tr>
<tr>
<td>Cisco Unified Mobile Communicator</td>
<td>30-10</td>
</tr>
<tr>
<td>Cisco Unified Mobility</td>
<td>30-9</td>
</tr>
<tr>
<td>interactions with Cisco Unified Mobility</td>
<td>14-29</td>
</tr>
<tr>
<td>license file</td>
<td></td>
</tr>
<tr>
<td>obtaining</td>
<td>30-13</td>
</tr>
<tr>
<td>sample license files</td>
<td>30-16</td>
</tr>
<tr>
<td>uploading</td>
<td>30-16</td>
</tr>
<tr>
<td>license unit report</td>
<td></td>
</tr>
<tr>
<td>generating</td>
<td>30-17</td>
</tr>
</tbody>
</table>
Index

more information 30-22
obtaining a software feature license 30-15
overview 30-1
phones 30-8
starting a license manager service 30-15
status notification 30-21
lines, interaction with MLPP 35-30
localizing calling party number
activating 8-15
BAT support 8-12
Call Detail Record support 8-12
calling party transformation CSS 8-25
calling party transformations patterns 8-7
CAR support 8-12
Cisco Extension Mobility support 8-13
Cisco Unified Communications Manager Assistant support 8-12
Cisco Unity Connection support 8-12
Cisco Unity support 8-12
configuration checklist 8-1
configuring 8-15
described 8-7
device mobility support 8-13
example 8-8
forwarding 8-11
information for end users 8-26
installing 8-15
interactions 8-11
mapping global number to local variant 8-9
phone support 8-10
related topics 8-27
restrictions 8-14
system requirements 8-10
transferring 8-11
local offnet access
managing in a centralized mode (figure) 31-6
local route groups
and called party transformations 31-11
and Cisco Unified Mobility 31-15
and forwarding 31-14
and route plan report 31-14
and supplementary services 31-14
binding a provisioned route group 31-4
called digits transformation (figure) 31-12
described 31-4
installing and activating 31-15
interactions 31-13
interactions and restrictions 31-13
interactions with Cisco Unified Mobility 14-29
introduction 31-3
mixed route list restrictions 31-15
overview 31-1
provisioning local offnet access with (figure) 31-8
provisioning local offnet access without (figure) 31-7
provisioning TEHO with (figure) 31-11
provisioning TEHO without (figure) 31-10
restrictions 31-15
routing with 31-5
simple local routing 31-6
supported devices 31-13
system requirements 31-13
with TEHO 31-9
location conveyance
across intercluster trunks 24-22
across SIP trunks 24-22
configuration 24-25
configuration checklist (table) 24-4
example PIDF-LO 24-24
feature interactions with midcall geolocation change 24-23
handling a received geolocation 24-23
intercluster trunk error handling for geolocation information 24-23
introducing 24-1, 24-21
related topics 24-25
SIP trunk error handling for geolocation information 24-22
logical partitioning
allow and deny policies 32-6
architecture overview 32-8  
configuration checklist (table) 32-1  
configuration upon upgrade 32-47  
configuring 32-39  
deny handling 32-18  
described 32-1  
device types and associated Cisco Unified CM devices (table) 32-5  
enterprise parameters 32-10  
feature interactions with midcall geolocation change 32-20  
geolocation configuration 32-39  
geolocation filter configuration 32-39  
geolocation identifiers  
usage 32-10  
geolocation usage for shared lines and route lists 32-10  
handling for basic call 32-19  
handling received geolocation identifiers 32-5  
interactions  
ad hoc conference, join, join across lines 32-27  
Barge, cBarge, Remote Resume 32-34  
call forwarding 32-23  
call park and directed call park 32-30  
call pickup 32-29  
call transfer 32-24  
Cisco Extension Mobility 32-31  
Cisco Unified Mobility 32-32  
CTI handling 32-36  
hunt pilots 32-35  
listed 32-22  
meet-me conference 32-28  
routing Lists 32-35  
shared lines 32-33  
interaction with dynamic SIP trunks 32-21  
interaction with geolocation conveyance across SIP  
and intercluster trunks 32-19  
introducing 32-4  
limitations 32-37  
LPPolicyManager 32-13  
LPSession infrastructure 32-18  
policies  
described 32-11  
example 32-11  
policy  
configuration settings (table) 32-43  
configuring 32-41  
deleting record 32-42  
finding 32-40  
policy checking 32-18  
policy configuration 32-40  
policy matching 32-17  
policy search algorithm  
example (table) 32-16  
explained 32-15  
policy tree  
described 32-13  
example (figure) 32-13  
related topics 32-47  
SIP or intercluster trunk configuration requirement 32-21  
system requirements 32-22  
TRAI regulations  
applicability 32-6  
history 32-7  
troubleshooting 32-47  
use of geolocations and geolocation filters 32-8  
login call flow  
Cisco Extension Mobility 9-9  
logout call flow  
Cisco Extension Mobility 9-10  
LPPolicyManager  
and logical partitioning 32-13  
LPSession infrastructure  
for logical partitioning 32-18
malicious call ID

adding a softkey template 33-8, 33-9
configuration checklist (table) 33-1
counting alarms 33-7
explained 33-2
feature code 33-3
giving MCID to users 33-8, 33-10
installing 33-6
interactions
alarms 33-5
call detail records 33-5
conference calls 33-5
extension mobility 33-5
listed 33-5
overview 33-2
related topics 33-11
removing MCID feature 33-9
restrictions 33-6
services 33-1, 33-3
setting service parameters 33-7
system requirements 33-3
troubleshooting 33-10
using 33-3

malicious call identification

supported devices 33-4

malicious call identification (MCID)

See malicious call ID

max list box enterprise parameter

calling search space 28-36

meet-me conference

interactions with logical partitioning 32-28

MGCP

and MLPP 35-32

MLPP

activating 35-41
announcements

blocked precedence 35-23

blocked precedence (figure) 35-23

busy station 35-24
explained 35-21

unauthorized precedence 35-22

unauthorized precedence (figure) 35-23

automated alternate routing (AAR) 35-32
call forward 35-30
call preservation 35-32
call transfer 35-31
call waiting 35-31

CDR recording 35-30
configuration checklist (table) 35-1
described 35-1
domain 35-9
enterprise parameters 35-42
hierarchical configuration 35-29
indication 35-12
installing 35-41
interactions 35-39
introducing 35-3
line feature interaction 35-30
mapping to DSCP 35-32
MGCP 35-32

numbering plan

example (figure) 35-25
explained 35-25

precedence

alternate party diversion (APD) 35-13
alternate party diversion example (figure) 35-14
call setup 35-12
explained 35-5
patterns 35-11
precedence patterns

example (figure) 35-25
explained 35-25

preemption

common network facility 35-17
common network facility example (figure) 35-18
common network facility example with retry timer
Trr (figure)  35-19
details  35-15
enabled  35-15
explained  35-8
receiving  35-15
user access  35-15
user access channel nonpreemptable  35-17
user access example (figure)  35-16
PRI  35-32
restrictions  35-39, 35-40
service parameter  35-29
shared lines  35-31
supplementary services
call forwarding  35-34
call pickup  35-36
call transfer  35-35
hunt pilots and hunt lists  35-36
multiple appearance lines  35-33
overview  35-33
three-way calling  35-35
terminology  35-4
trunk selection
example (figure)  35-28
explained  35-26
mobile connect
and MLPP  14-27, 15-18
feature interactions  14-27, 15-18
overview  14-4
related topics  14-62, 15-20
restrictions  14-27, 15-18
mobile voice access
configuration settings (table)  14-49
directory number  14-48
overview  14-4, 15-4
related topics  14-62, 15-20
mobility softkeys
configuring  14-61
modifying files  19-2
MOH
See music on hold (MOH)
monitoring
adding user for application (figure)  34-64
adding user to groups (figure)  34-65
agent call  34-12
agent cannot control a monitoring call (figure)  34-10
agent conferences in the supervisor (figure)  34-14
agent in a conference (figure)  34-13
architecture (figure)  34-4
BIB  34-58
call characteristics  34-55
call information  34-58
call preservation  34-58
codec for calls (figure)  34-56
configuration checklist (table)  34-1
configuring  34-63
configuring calling search spaces (figure)  34-67
configuring tones (figure)  34-66
CTI event delivery (figure)  34-59
CTI requirements  34-59
described  34-1
firewalls (figure)  34-57
hardware requirements  34-60
interactions listed  34-60
interactions with CTI and JTAPI/TSP applications  34-60
interactions with other features  34-61
introducing  34-2, 34-8
invocation of a session  34-8
IPv6  29-19
limitations
listed  34-61
multiple sessions (figure)  34-12
notification tones  34-55
one-way media  34-57
one-way media (figure)  34-57
play tone behavior  34-55
related topics  34-75
restrictions
  security 34-62
  with intercom 34-62
service parameters 34-74
session (figure) 34-9
session flow (figure) 34-8
simultaneous with recording (figure) 34-54
streaming through the agent IP phone (figure) 34-6
supervisor conferences in another supervisor (figure) 34-15
supervisor transfers the monitoring call (figure) 34-10
supported devices 1-11, 20-9, 21-4, 34-6
system requirements 34-59
terminology 34-3
turn on IP phone BIB to allow (figure) 34-64

MTP
  IPv6 29-12
multicast
  audio sources for MOH 36-13
  configuration checklist (table) 36-3
  explained 36-13
multilevel precedence and preemption
  See MLPP
  supported devices 35-38
  system requirements 35-38
music on hold
  IPv6 29-19
music on hold (MOH)
  audio files
    deleting 36-35
    displaying 36-33
    managing 36-33
    uploading 36-34
  audio sources
    configuration settings (table) 36-21
    configuring 36-18, 36-20
    deleting 36-21
    explained 36-12
    finding 36-19

call park example 36-8
characteristics 36-6
configuration checklist (table) 36-1
creating audio sources 36-12
database scalability 36-10
definitions 36-4
described 36-1
failover and fallback 36-18
features
  manageability 36-10
  server manageability 36-9
  server redundancy 36-9
  server scalability 36-9
fixed audio source
  configuration settings (table) 36-25
  configuring 36-24
  deleting 36-24
  described 36-23
functionality 36-7
list of topics 36-1
managing audio sources 36-13
monitoring performance
  overview (table) 36-4
  service states 36-36
requirements and limits 36-16
server configuration settings (table) 36-28
servers
  characteristics 36-8
  configuring 36-25, 36-27
  database requirements 36-10
  explained 36-11
  finding 36-26
  manageability 36-9
  perfmon counters 36-36
  redundancy 36-9
  resetting 36-27
  scalability 36-9
  synchronizing configuration 36-28
  storing audio sources 36-12
supported features 36-8
transfer hold example 36-8
understanding 36-4
user hold example 36-8

N
nonpreemptable user access channel 35-17
notification tones for monitoring and recording 34-55
numbering plan
MLPP (figure) 35-25
MLPP access control 35-25

O
other group pickup
configuration checklist (table) 6-3
described 6-12

P
parameters, service
CDR 33-7
park monitoring 5-16
    directory number configuration window 5-18
    setting service parameters 5-16
partitions
restricting access 6-21
    using call pickup 6-21
    Web Dialer support 17-11
party entrance tone
    barge, cBarge, single button barge 1-9
PCM file requirements for custom ring types 19-3
perfmom counters
    counter descriptions (table) 36-36
    using to view MOH servers 36-36
phones
    and call display restrictions 4-8
custom rings
    creating 19-1, 19-3
    overview 19-1
    PCM file requirements 19-3
    interaction with Presence 37-5
IPv6 and web browser 29-20
licensing 30-8
physical locations
    configuration settings (table) 20-14
    configuring 20-13
deleting 20-15
finding 20-12
PIDF-LO
    example 24-24
PLAR
    for barge, cBarge, and single button barge 1-13
policies
    logical partitioning
        described 32-11
        example 32-11
    policy
        checking
            for logical partitioning 32-18
        configuration for logical partitioning 32-40
    logical partitioning
        configuration settings (table) 32-43
        configuring 32-41
deleting record 32-42
finding 32-40
matching 32-17
    variations in policy configuration (table) 32-16
policy search algorithm
    for logical partitioning (table) 32-16
    explained 32-15
policy tree
    for logical partitioning 32-13
    logical partitioning (figure) 32-13
preference
alternate party diversion (APD)
  example (figure) 35-14
  explained 35-13
blocked 35-23
blocked (figure) 35-23
busy station 35-24
call setup 35-12
CDR recording 35-30
explained 35-5
patterns
  access control 35-25
  MLPP (figure) 35-25
  setup 35-11
unauthorized 35-22
unauthorized (figure) 35-23
preemption
  common network facility 35-17
  common network facility example (figure) 35-18
  common network facility example with retry timer Trr (figure) 35-19
details 35-15
enabled 35-15
explained 35-8
receiving 35-15
user access 35-15
user access channel nonpreemptable 35-17
user access example (figure) 35-16
Presence
  authorization 37-9
BLF/SpeedDial
  buttons, configuring 37-20
  configuration settings (table) 5-27, 37-21
  configuring 37-20
configuration checklist (table) 37-1
feature interactions and restrictions 37-12
groups
  applying 37-18
  configuration example 37-8
  configuration settings (table) 37-17
explained 37-7
interaction examples 37-9
interaction with Cisco Extension Mobility 37-11
interaction with phones and trunks 37-5
interaction with route lists 37-6
more information 37-22
overview 37-1, 37-4
request examples 37-5
SUBSCRIBE calling search space 37-11, 37-14
tips for presence group and presence authorization 37-19
PRI and MLPP 35-32
privacy
  activating 1-16
  configuration checklist (table) 1-4
  configuring 1-17
  described 1-10
  installing and activating 1-16
  interactions and restrictions 1-12
  overview 1-1
  related topics 1-17
  service parameters 1-17
  system requirements 1-11
privacy on hold
  activating 1-16
  configuration checklist (table) 1-4
  configuring 1-17
  described 1-10
  installing and activating 1-16
  interactions and restrictions 1-12
  related topics 1-17
  service parameters 1-17
  system requirements 1-11
proxy user, creating for Web Dialer 17-12

Q
QRT
activating 38-15
activating CEF service 38-22
adding softkey template to phones 38-20
alarms and traces 38-22
architecture overview 38-4
can’t make calls (figure) 38-14
can’t make calls (table) 38-14
Cisco Extended Functions service 38-7
components 38-3
configuration checklist (table) 38-2
configuring 38-16
configuring softkey template in common device configuration 38-19
creating softkey template 38-17
description 38-3
extended menu choices 38-10
information to users 38-30
installing 38-15
interactions 38-9
IP phone support 38-6
IPv6 29-19
overview 38-1
phone configuration (figure) 38-21
phone interface (figure) 38-11
phone interface display (figure) 38-10
phone recently rebooted (table) 38-13
problem categories (table) 38-11
problems with last call (table) 38-13
problem with phone that recently rebooted (figure) 38-14
QRT Viewer 38-25
reason codes (table) 38-11
related topics 38-32
reporting problem with current call (figure) 38-12
reporting problem with last call (figure) 38-13
reports
  described 38-26
  fields by supported category 38-28
restrictions 38-15
securing signaling connections 38-8
serviceability features 38-21
setting service parameters 38-24
softkey 38-17
softkey layout configuration (figure) 38-19
softkey template configuration window (figure) 38-17
softkey template configuration window after copy (figure) 38-18
system requirements 38-6
troubleshooting 38-30
user interface 38-9
using 38-9
voice quality feedback (figure) 38-10
Quality Report Tool (QRT)
  See QRT

R

recording
  adding user for application (figure) 34-64
  adding user to groups (figure) 34-65
  agent conference (figure) 34-52
  application-invoked 34-17
  application-invoked (figure) 34-49
  architecture (figure) 34-4
  automatic 34-17
  automatic (figure) 34-19
  barged call (figure) 34-52
  BIB 34-58
  call characteristics 34-55
  call display 34-58
  call information 34-58
  call preservation 34-58
  calls do not survive agent hold (figure) 34-50
  codec for calls (figure) 34-56
  configuration checklist (figure) 34-1
  configuring 34-63
  configuring calling search spaces (figure) 34-67
  configuring tones (figure) 34-66
creating a route pattern for the recorder (figure) 34-72
creating recorder redundancy (figure) 34-73
creating SIP trunk that points to the recorder (figure) 34-71
CTI event delivery (figure) 34-59
CTI requirements described 34-1
enabling for a line appearance (figure) 34-68
firewalls (figure) 34-57
hardware requirements 34-60
interactions listed 34-60
interactions with CTI and JTAPI/TSP applications 34-60
interactions with other features 34-61
introducing 34-2, 34-16
IPv6 29-19
limitations listed 34-61
limiting codec usage 34-56
modes 34-17
notification tones 34-55
one-way media 34-57
one-way media (figure) 34-57
overview (figure) 34-3
play tone behavior 34-55
profiles creating (figure) 34-69
recorder as SIP trunk device 34-18
related topics 34-75
restrictions security 34-62
with intercom 34-62
service parameters 34-74
simultaneous with monitoring (figure) 34-54
streaming through the agent IP phone (figure) 34-6
supported devices 1-11, 20-9, 21-4, 34-6
system requirements 34-59
terminology 34-3
turn on IP phone BIB to allow (figure) 34-64
Redirector servlet configuring 17-11
redundancy creating for recorders (figure) 34-73
MOH servers 36-9
Web Dialer 17-3
remote destination profiles associating a directory number 14-43
configuration 14-39
configuration settings (table) 14-39
remote destinations configuration settings (table) 14-44
configuring 14-43
intelligent session control 14-17
Remote Resume interactions with logical partitioning 32-34
requirements
Call Back 2-6
Cisco Extension Mobility 9-13
Cisco Unified Mobility 14-34
with Cisco Unified Mobility Advantage 15-19
device mobility 20-9
hold reversion 25-8
retry timer Trr example (figure) 35-19
reverse callback dial-via-office with Cisco Unified Mobility 15-10
reverted calls 25-5
Ringlist.xml file format 19-2
route groups binding to a local route group 31-4
local
and called party transformations 31-11
and forwarding 31-14
and route plan report 31-14
and supplementary services 31-14
binding a provisioned route group 31-4
called digits transformation (figure) 31-12
described 31-4
installing and activating 31-15
interactions 31-13
introduction 31-3
mixed route list restrictions 31-15
provisioning local offnet access with (figure) 31-8
provisioning local offnet access without (figure) 31-7
provisioning TEHO with (figure) 31-11
provisioning TEHO without (figure) 31-10
restrictions 31-15
routing with 31-5
supported devices 31-13
system requirements 31-13
route lists
and geolocations 24-8
interactions with logical partitioning 32-35
interaction with Presence 37-6
logical partitioning geolocation usage 32-10
route patterns
creating for the recorder (figure) 34-72
route plan report
and local route groups 31-14
routing
simple with local route groups 31-6
RSVP
IPv6 29-19

S

SAF 3-1
SCCP
status notification for DND 21-3
security
Cisco Unified Communications Manager Assistant 11-28, 12-19
IPMASecureSysUser 11-28, 12-19
Presence authorization 37-9
with monitoring feature 34-62
with recording feature 34-62
service parameters

barge 1-17
CDR 33-7
external call transfer restrictions 23-7
for call pickup 6-26
for Cisco Extension Mobility (table) 9-20
for monitoring and recording 34-74
for recording and monitoring (figure) 34-67
MLPP 35-29
Presence 37-13
privacy 1-17
privacy on hold 1-17
Web Dialer 17-6

services
adding the Cisco Extension Mobility service 9-19
supplementary for MLPP 35-33
shared conference bridges and cBarge 1-16
shared lines
and geolocations 24-8
interactions with logical partitioning 32-33
logical partitioning geolocation usage 32-10
MLPP interaction 35-31
single button barge
party entrance tone 1-9
PLAR support 1-13

single sign on
CLI commands 39-5
configuration checklist (table) 39-1
configuring 39-3
configuring client browsers 39-4
configuring FireFox 39-5
configuring Internet Explorer 39-5
configuring OpenAM 39-3
configuring Windows single sign on with Active Directory and OpenAM 39-4
described 39-2
importing OpenAM certificates 39-4
installing and activating 39-3
overview 39-1
related topics 39-7
system requirements 39-2
utils sso disable CLI command 39-6
utils sso enable CLI command 39-5
utils sso status CLI command 39-7
SIP
  DND status notification 21-3
  recorder as SIP trunk device 34-18
  trunks
     creating to point to the recorder (figure) 34-71
  URI dialing with Cisco Unified Mobility 14-16
SIP trunks
  configuration requirement for logical partitioning 32-21
  interactions with logical partitioning 32-21
IPv6 29-13
  location conveyance 24-22
  logical partitioning interaction with geolocation conveyance 32-19
softkeys
  barge 1-8
cBarge 1-9
  configuring mobility 14-61
  templates for MCID 33-8, 33-9
SRST
  intercom usage 28-6
supplementary services
  call forwarding 35-34
  call pickup 35-36
  call transfer 35-35
  hunt pilots and hunt lists 35-36
  multiple appearance lines 35-33
  overview 35-33
  three-way calling 35-35
system remote access
  H.323 configuration
     no hairpinning 14-50
     using hairpinning 14-53
  system requirements
     call pickup 6-22
T
  T.38 Fax
     IPv6 29-20
  tail end hop off (TEHO)
     and local route groups 31-9
  TEHO
     and local route groups 31-9
  templates, softkey
     MCID 33-8, 33-9
TFTP
  IPv6 29-15
time-of-day access
  with Cisco Unified Mobility
     configuration checklist (table) 14-13
     described 14-12
     important notes 14-14
TLS, securing connection to CTI 38-8
trace settings, Web Dialer 17-14
transfer
  external call transfer restrictions 23-1
  IPv6 29-20
  transfer hold, example with MOH 36-8
  transformations
     called party with local route groups 31-11
  translation patterns
     for call display restrictions 4-7
Trr retry timer preemption example (figure) 35-19
trunks
  interaction with Presence 37-5
  IPv6 and SIP trunks 29-13
  selection for MLPP
     example (figure) 35-28
     explained 35-26
U
unicast
  audio sources for MOH 36-13
explained  36-13

URI
dialing with Cisco Unified Mobility  14-16
user hold, example with MOH  36-8

V

video
IPv6  29-20
voice mail
interaction with call display restrictions  4-6

W

Web Dialer
activating  17-5
adding users to standard Cisco Unified Communications Manager end users group  17-12
configuration checklist (table)  17-1
configuring  17-6
configuring application dial rules  17-11
configuring for local language  17-10
configuring Redirector servlet  17-11
creating a proxy user  17-12
installing  17-5
interactions  17-4
interactions and restrictions  17-4
introducing  17-2
locale settings in Microsoft Internet Explorer (figure)  17-10
overview  17-1
partition support  17-11
redundancy  17-3
related topics  17-14
restrictions  17-5
secure TLS connection  17-9
service parameters  17-6
servlet
   Redirector  17-3

Webdialer  17-2, 17-6
system requirements  17-4
trace settings  17-14